NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPLORING DATA SHARING BETWEEN GEOGRAPHICALLY DISTRIBUTED MOBILE AND FIXED NODES SUPPORTING EXTENDED MARITIME INTERDICTION OPERATIONS (EMIO)

by

Albert Mercado

June 2008

Thesis Advisor: Alex Bordetsky
Second Reader: Eugene Bourakov

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2.REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Exploring Data Sharing Between Geographically Distributed Mobile and Fixed Nodes Supporting Extended Maritime Interdiction Operations (EMIO)			**5. FUNDING NUMBERS**
6. AUTHOR(S) LT Albert Mercado			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

After the 9/11 catastrophe, insurgents and terrorists have shown us that they will continue to employ asymmetric threats to carry out their objectives, by using any available equipment or any available route to their objective that remains unchecked or unchallenged, like car bombs, suicide bombers, and commercial airplanes. In response, the United States and its allies are focusing harder on data sharing efforts in order to improve the situational awareness (SA) of command and control (C2) structures, to make quicker decisions, and to collaborate with remote experts on chemical, biological, and radiological elements, biometrics, or explosive devices.

This thesis discusses the data sharing contributions and features of collaborative tools used onboard a boarding vessel in a riverine area and participating nodes to provide or to enhance the SA and decision making process during EMIOs. As maritime operational experiments, conducted by the Center for Network Innovation and Experimentation (CENETIX), are more successful with each successive MIO experiment, a better understanding for methods of sharing substantial data captured during these operations with participating nodes will be reached.

14. SUBJECT TERMS Wireless, MIO, Networks, Situational Awareness, Tactical Operations Center, Command and Control, Nodes, Data sharing, Riverine, CENETIX			**15. NUMBER OF PAGES** 127
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

EXPLORING DATA SHARING BETWEEN GEOGRAPHICALLY DISTRIBUTED MOBILE AND FIXED NODES SUPPORTING EXTENDED MARITIME INTERDICTION OPERATIONS (EMIO)

Albert Mercado
Lieutenant, United States Navy
B.A., University of Houston, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author: Albert Mercado

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Eugene Bourakov
Second Reader

Dan C. Boger
Chairman, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

After the 9/11 catastrophe, insurgents and terrorists have shown us that they will continue to employ asymmetric threats to carry out their objectives, by using any available equipment or any available route to their objective that remains unchecked or unchallenged, like car bombs, suicide bombers, and commercial airplanes. In response, the United States and its allies are focusing harder on data sharing efforts in order to improve the situational awareness (SA) of command and control (C2) structures, to make quicker decisions, and to collaborate with remote experts on chemical, biological, and radiological elements, biometrics, or explosive devices.

This thesis discusses the data sharing contributions and features of collaborative tools used onboard a boarding vessel in a riverine area and participating nodes to provide or to enhance the SA and decision making process during EMIOs. As maritime operational experiments, conducted by the Center for Network Innovation and Experimentation (CENETIX), are more successful with each successive MIO experiment, a better understanding for methods of sharing substantial data captured during these operations with participating nodes will be reached.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Report
AP	Access Point
ARAM	Adaptable Radiation Area Monitor
BFC	Biometrics Fusion Center
BFT	Blue Force Tracker
BO	Boarding Officer
BP	Boarding Party
BV	Boarding Vessel
C2	Command and Control
CB	Chase Boat
CBRN	Chemical, Biological, Radiological, Nuclear
CCRP	The Command and Control Research Program
CENETIX	Center for Network Innovation and Experimentation
CONUS	Continental United States
COP	Common Operating Picture
COTS	Commercial Off-the-Shelf
CWMD	Combating Weapons of Mass Destruction
DM	Decision Makers
DoD	Department of Defense
DTRA	Defense Threat Reduction Agency
DU	Depleted Uranium
EAL	Evaluation Assurance Level
ELINT	Electronic Intelligence

EMIO	Extended Maritime Interdiction Operation
FBI	Federal Bureau of Investigations
FIPS	Federal Information Processing Standard
GGB	Golden Gate Bridge
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HIS	Human System Integration
HLS	Homeland Security
HQ	Headquarters
HVT	High Value Target
ICMP	Internet Control Message Protocol
IM	Instant Messaging
IMU	Inertial Magnetic Unit
IST	Innovative Survivability Technologies
JSA	Joint Situational Awareness
LAN	Local Area Network
LBNL	Lawrence Berkley National Laboratories
LLNL	Lawrence Livermore National Laboratories
LLWO	Lawrence Livermore Watch Officer
LOS	Line of Sight
LRV	Land Reconnaissance Vehicle
MHz	Megahertz
MIB	Management Information Base (for SNMP)
MIFC	Maritime Intelligence Fusion Center

MIMO	Multiple Input Multiple Output
MIO	Maritime Interdiction Operations
MOTR	Maritime Operational Threat Response
MSST	Maritime Safety and Security Team
MU	Marine Unit
NLOS	Near Line of Sight
NNSA	National Nuclear Security Administration
NOC	Network Operations Center
NORM	Naturally Occurring Radioactive Materials
NPS	Naval Postgraduate School
NRC	National Response Center
NRL	Naval Research laboratory
NY	New York
OFDM	Orthogonal Frequency Division Multiplexing
OPAREA	Operational Area
PANYNJ	Port Authority New York New Jersey
RAP	Radiological Assistance Program
RHIB	Rigid Hull Inflatable Boat
RFI	Radio Frequency Interference
SA	Situational Awareness
SAOFDM	Self-Aligning Orthogonal Frequency Division Multiplexing
SATCOM	Satellite Communications
SF	San Francisco
SFPD	San Francisco Police Department
SMS	Short Messaging System

SNMP	Simple Network Management Protocol
SNWC	Swedish Naval Warfare Center
SOHO	Small Office Home Office
TACSAT	Tactical Satellite
TNT	Tactical Network Topology
TOC	Tactical Operations Center
TV	Target Vessel
UGV	Underground Vehicle
URL	Uniform Resource Locator
USB	Universal Serial Bus
USCG	United States Coast Guard
USDOE	United States Department of Energy
USDOJ	United States Department of Justice
USSOCOM	United States Special Operations Command
USV	Unmanned Surface Vehicle
UWB	Ultra Wideband
VAC	Voltage Alternating Current
VC	Video Conference
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access
WMD	Weapons of Mass Destruction
YBI	Yerba Buena Island

ACKNOWLEDGEMENTS

First and most, I would like to thank God for helping me in this endeavor. His intervention had to be in everything I did, otherwise, I would not have succeeded. It is for His glory that I do everything I can to be a better Christian in this world.

I would like to thank Dr. Bordetsky and Mr. Eugene Bourakov for their strong support and encouragement throughout my participation and work in the CENETIX, Camp Roberts, and San Francisco. Their strong guidance helped me understand the research that goes on behind the technology that the military employs to give our war fighters the cutting edge in any conflict.

I would also like to thank my wife, Rocio, and my son, Albert, for their help and patience while I attended NPS. Their strong encouragement and commitment to helping me succeed made me realize that no one can achieve major goals without the support of their family. Rocio and Albert, I love you.

Finally, I would like to thank my parents and siblings for giving me some words of encouragement throughout my studies at NPS. They made me realize that we still rely on each other's moral support to keep moving ahead.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Time, space, and force are factors which affect the outcome of any confrontation between opposing forces. Years before the 9/11 attacks on American soil, asymmetric threats have been employed by terrorists to achieve their objectives by using car bombs or suicide bombers. Even though riverine areas have not seen great action since the Viet Nam War, in March 2006, the United States Department of Justice (USDOJ) recognized the efforts of the Federal Bureau of Investigation to protect our nation's seaports. In the Audit Report 06-26 from the Office of the Inspector General, March 2006, the following facts were recognized.

- 95 percent of overseas trade flows through the more than 360 seaports and inland waterways of the United States.
- Large metropolitan areas and hazardous chemical storage facilities within short range of these seaports can become vulnerable terrorist's targets.
- According to the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), maritime terrorism has the same or higher probability to occur as aviation terrorism.
- The Maritime Operational Threat Response (MOTR) plan supports the National Strategy for Maritime Security.

Therefore, it is necessary for foreign and domestic military and civilian maritime interdiction forces to work together by sharing data through common collaborative tools in order to dominate the information domain to meet or surpass any asymmetric threats from terrorists or counterinsurgents in the maritime environment. Furthermore, due to their complex environment, riverine areas provide terrorists or criminals the route they need to clandestinely move around anything or anyone. Riverine areas include any river

or littoral body of water. In some areas of the world, the riverine areas are further complicated by the amount of civilian traffic flowing through it or the surrounding terrain.

To add to this dilemma of high civilian maritime traffic, the time spent processing every possible target vessel or suspect can easily give the opposing force the advantage of escaping through riverine maritime interdiction forces facing multiple targets. Furthermore, every boarding by maritime interdiction forces is complicated by copious amounts of data sharing between the interdiction force and remote supporting agencies, assistance centers, or experts. To counteract this dilemma in both domestic and foreign locations, maritime interdiction forces must improve the situational awareness (SA) of command and control (C2) structures through data sharing capabilities and data management resources that will enable them to quickly confront every suspected threat without losing efficiency.

In past Maritime Interdiction Operations, communications between the BP and boarding vessel were established via standard two-way walkie-talkie radios. (Marvin, 2005) Furthermore, the BP was very slow to capture, send, and process data. Real-time collaboration with C2 elements and participating agencies was not available, since all data was hand-written by the BP, transmitted to the boarding vessel via radio talker, rewritten on another report, and then incorporated with other data into a message to the Maritime Interdiction Operation Warfare Commander via DoD SATCOM. (Marvin, 2005) This manpower intensive and time-wasteful method of sharing data gives substantial reason to why real-time collaborative tools need to be incorporated into MIO experiments.

In order to provide expeditious data sharing from a mobile wireless node placed onboard a riverine unit, an ad-hoc network reaching from the riverine unit back to the Tactical Operations Center (TOC) has to be established and supported by collaborative tools to enhance the SA of all MIO participants. The Navy has a long history of using various coordination methods using VHF handheld radios to establish communications between riverine assets and operation centers in order to find riverine-based criminals or terrorists and execute maneuvers or plans to capture these targets. Currently, the VHF

handheld radios are still used only to provide a redundant line of communications between the BP and boarding vessel. However, as years have gone by since the inception of these kinds of operations, new network technology and collaborative tools have been implemented for faster and more reliable data sharing to improve the decision-making process.

In recent years, wireless technology and collaborative tools have made a huge leap into society. As such, maritime interdiction forces operating in riverine areas have been able to keep up with these capabilities to explore and to exploit its advantages in order to establish and expedite data sharing with operation centers and remote experts. The objective of The Tactical Network Topology Maritime Interdiction Operations "was to continue to evaluate the use of networks, advanced sensors, and collaborative technology for rapid Maritime Interdiction Operations; specifically, the ability for a Boarding Party (BP) to rapidly set up ship-to-ship communications that enable the BP to search for radiation and explosive sources. The necessity to maintain network connectivity with command and control (C2) elements and collaborating with remotely located sensor experts were also key objectives." (TNT 07-4 AAR)

During past TNT MIO experiments, data sharing tools have been employed to raise the SA of participating nodes and to include inputs from remote experts in the continental United States (CONUS), which have the facilities or capabilities to further analyze captured data, in order to expedite the decision-making process. Quarter by quarter, TNT MIO experiments have evolved to become more operationally realistic and complex by including substantial data from radiation sensors and biometric devices coupled with geographically distributed support agencies and participants, who can bring substantial intelligence about the MIO scenario. This thesis will examine the evolution of the data sharing aspect of MIO experiments driven by the CENETIX at NPS. Furthermore, this thesis will attempt to determine if one data sharing tool alone can handle or surpass the SA requirements for expeditious decision-making among the riverine unit, the TOC, and geographically distributed supporting nodes.

B. OBJECTIVES

The objectives of this study are to examine:

- How the data sharing tools explored in previous experiments contributed to the decision-making process under more diverse operational conditions in the Monterey and San Francisco bay areas.
- How the data sharing tools contributed to the decision-making process during the recent TNT MIO 08-2 experiment under operational conditions.
- The features to improve upon the data sharing contributions for future experiments conducted under more complex operational conditions.

C. RESEARCH TASKS

1. Data Sharing Requirements

- What features should the collaborative tools provide in order to meet or to enhance the SA and data sharing contributions of all participating nodes in an operational environment?
- What kind of data is going to be shared through the collaborative tools, i.e. files, video, chat, radiation sensor data, and through what equipment, i.e. video conference equipment or flash drive downloads?
- How is data sharing going to improve or to expedite the boarding officer's and TOC's decision-making process during the EMIO?

2. Remote Experts Data Sharing Capabilities

- Which data sharing tools are available for remote experts included in the MIO network to provide a route and feedback of captured data or to interact with geographically distributed participants?
- How did the data sharing occur in geographically distributed sites between the riverine area, open bay, and open waters?

- Which data sharing tasks may be automated to eliminate human-in-the-loop data exchange process?

D. SCOPE

The scope of this thesis is to discuss the contributions and features of collaborative tools in MIO networks in operational conditions to improve the SA and decision-making process of all involved MIO participants.

E. METHODOLOGY

Previous TNT MIO experiments will provide a background of information on the contributions and expectations of data sharing tools. By comparing previous results with TNT MIO 08-2 data sharing results, specifically in the riverine area, the collaborative tools can be further examined to recommend improvements.

F. THESIS ORGANIZATION

This thesis is organized as follows. Chapter II describes remote experts, data sharing tools, and types of shared data. Chapter III summarizes the data sharing environment in past MIO experiments. Chapter IV describes the data sharing aspect of the recent TNT MIO 08-2 experiment in the riverine area and its results. Chapter V discusses the conclusion. Chapter VI describes future recommendations for upcoming riverine experiment.

THIS PAGE INTENTIONALLY LEFT BLANK

II. REMOTE EXPERTS, DATA SHARING TOOLS, AND TYPES OF DATA

A. CONTRIBUTIONS OF REMOTE EXPERTS

1. Lawrence Livermore National Laboratories (LLNL)

The purpose of LLNL, with respect to the MIO operational experiments conducted, is to provide remote expert intelligence about the sensor data captured during a MIO and provide the TOC or BP feedback or recommendations for further analysis by their experts. Due to the limited personnel which comprise a BP, none of which are scientists, at this time, a near real-time reach back must provide the BP and the TOC a route for crucial information sharing needed to decide whether or not a suspected target vessel is carrying nuclear material.

To further assist the expeditious inspection of the target vessel or simply give the maritime interdiction forces the opportunity to deter a target vessel from penetrating from international into territorial or even riverine waters, the LLNL has two types of equipment which help in the detection of nuclear material. If the target vessel (TV) is emitting nuclear radiation to the environment, whether or not the TV is capable of traveling in Riverine waters, the LLNL has an exterior-mounted sensor, which can pick up the emitted radiation, when it drives within a close range of the TV. This ARAM sensor can be used more appropriately in inland waters due to the nature of traffic flow and traffic scheme. Otherwise, at close range in open ocean waters, a large TV is capable of travelling at dangerous speeds for a comparably smaller maritime interdiction vessel to pick up any nuclear radiation without keeling over from the Coriollis effect developed between the two vessels.

Since “radioactive material is everywhere from the concrete in our streets to the food we eat,” if a large vessel is suspected of carrying nuclear material, but is not radiating out into the environment towards any LLNL radiation sensor, then the other type of LLNL sensor applies. (Dougan, 2004) This handheld sensor, appropriately

called the IdentiFINDER, is used by BP personnel during their more intricate inspection of the TV's interior and topside spaces. The data collected from these locally implemented radiation sensors have to be provided with a real-time path back to the LLNL for further analysis and successive handling instructions from the laboratory. Without the prompt analysis of radiation data captured locally, maritime vessels can be detained indefinitely and unnecessarily from something as simple as a smoke detector, which holds in it Americum-241. (Dougan, 2004) Thus, this is why the LLNL must be a remote collaborating expert included as a node in the EMIO network topology.

Furthermore, LLNL officials respond regularly when local Customs and Coast Guard officials at the San Francisco Airport and the Port of Oakland receive unusual alerts on their radiological pagers. The Lab has field-tested a number of portable radiation monitors at both locales to assist in the detection of weapons of mass destruction. In addition, LLNL is working closely with the California Highway Patrol to develop additional radiation detection technology to prevent smuggling of radioactive material into the State.

Figure 1. Adaptable Radiation Area Monitor
(From Dougan, 2003)

2. Biometrics Fusion Center (BFC)

The Biometrics Fusion Center, located in Clarksburg, West Virginia, is a remote expert in these MIO experiments, which can provide the intelligence derived from biometric data collected at the tactical level of operations. Established in December 2000, the BFC performs various biometrics field researches, of which biometric repository support to the Department of Defense (DoD) is the most important to EMIO. One of its core functions includes establishing and maintaining an authoritative biometric data source in order to provide timely, accurate and comprehensive Identity Superiority to the war fighter, which in this case are the MIO TOC personnel. (WV Biometrics Initiative Website, 2008) Therefore, even when a new suspect or criminal is apprehended, the BP must be able to quickly send biometric data to the BFC in order to update their database. To achieve this objective, it is necessary to include the BFC and any linking nodes in the EMIO network.

3. United States Coast Guard

The Coast Guard, as part of the Department of Homeland Security, reports directly to the Secretary of Homeland Security. However, upon the declaration of war and when Congress or the President directs, the Coast Guard operates under the Department of Defense as a service in the Department of the Navy. Under 14 U.S.C. Section 2 the Coast Guard is authorized to enforce federal law. Furthermore, the Coast Guard is exempt from and not subject to the restrictions of the Posse Comitatus Act which restrict the law enforcement activities of the other four military services within United States territory. (Wikipedia, 2008)

Operated by the U.S. Coast Guard, the National Response Center (NRC) is the sole U.S. Government point of contact for reporting environmental spills, contamination, and pollution. The primary function of the National Response Center (NRC) is to serve as the sole national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment anywhere in the United States and its territories. The NRC maintains agreements with a variety of federal

entities to make additional notifications regarding incidents meeting established trigger criteria. The NRC also takes Terrorist/Suspicious Activity Reports and Maritime Security Breach Reports. (USEPA Website, 2007)

4. Federal and Local Law Enforcement Agencies

- The Federal Bureau of Investigations (FBI) has a database called the Guardian Threat Tracking System (Guardian), which holds information on maritime and other terrorist threats and suspicious incidents.
- Oakland, San Francisco, and Sacramento maritime interdiction forces collaborate with each other and with USCG to provide the manpower, intelligence reports, and interdiction tactics to further assist the C2 elements in finding maritime terrorists or HVTs.
- The mission of the Defense Threat Reduction Agency is to reduce the threat to the United States and its allies from nuclear, biological, chemical weapons, other special weapons, and conventional weapons, through the execution of technology security activities, cooperative threat reduction programs, arms control treaty monitoring and on-site inspections, force protection, nuclear, biological, chemical defenses, and counter-proliferation. (Harahan & Bennett, 2002) As a combat support agency, founded in 1998 at Fort Belvoir, Virginia, under the U.S. Department of Defense, it is composed of three enterprises, which include Combating Weapons of Mass Destruction (CWMD) Enterprise, Operations Enterprise, and Research and Development Enterprise. It is the DTRA's CWMD Enterprise's technical support in MIOs that makes them a valuable asset to incorporate in the decision making process when WMDs are involved.

5. Naval Research Laboratory (NRL)

The NRL provides Tactical Satellite (TACSAT) capabilities to local and remote government agencies. During the experiments, the NRL provided imaging of Monterey bay and radiation spectrum files to LLNL.

6. Maritime Intelligence Fusion Center (MIFC)

The role of MIFC is to provide maritime traffic information such as ships' registries, cargo and crew manifests, ports of call, and shipping schedules. This information is helpful in order to designate a vessel as suspect, locate it, make its interdiction possible, and confirm discrepancies onboard, such as fake documentation. (Stavroulakis, 2006)

7. United States Department of Energy (USDOE)

Under the USDOE, the National Nuclear Security Administration (NNSA) handles worldwide radiological accidents and incidents through various assets, one of which is the Radiological Assistance Program (RAP). RAP is one of NNSA's first responders for assessing situations to minimize hazards of a radiological emergency through assessment, area monitoring, air sampling, and exposure and contamination control. Able to arrive within four to six hours of notification of a radiological emergency, RAP personnel use state-of-the-art equipment to help identify or minimize radiological hazards. (RAP, 2008)

8. Coalition Partners

Coalition partners are involved in the experiments to bring in a geographically distributed node perspective in the MIO experiments conducted with operational conditions. Austria, Sweden, and Singapore have been greatly involved with the San Francisco MIO experiments conducted in collaboration with CENETIX, NRL, USCG District 11, LLNL, LBNL, BFC, MIFC, DTRA, and local maritime interdiction forces from San Francisco, Oakland, and Sacramento in order to better evaluate the geographically distributed collaboration of MIOs using rapidly-deployed wireless

networks and collaborative tools to augment pre-established wireless backbones, databases, VPN, and public internet access. Through their participation in the MIO experiments, a better commitment to understanding how international participants help to provide data necessary to evaluate a MIO situation involving terrorists, radiation materials, or WMDs

B. DATA SHARING TOOLS

1. GROOVE V3.0

The following MIO pertinent features are available in the Groove V3.0 software.

- Contact Manager- to create a list of shared contacts
- Discussion- to discuss topics within the workspace
- Document Review- to review documents in the workspace
- Files- to manage shared files

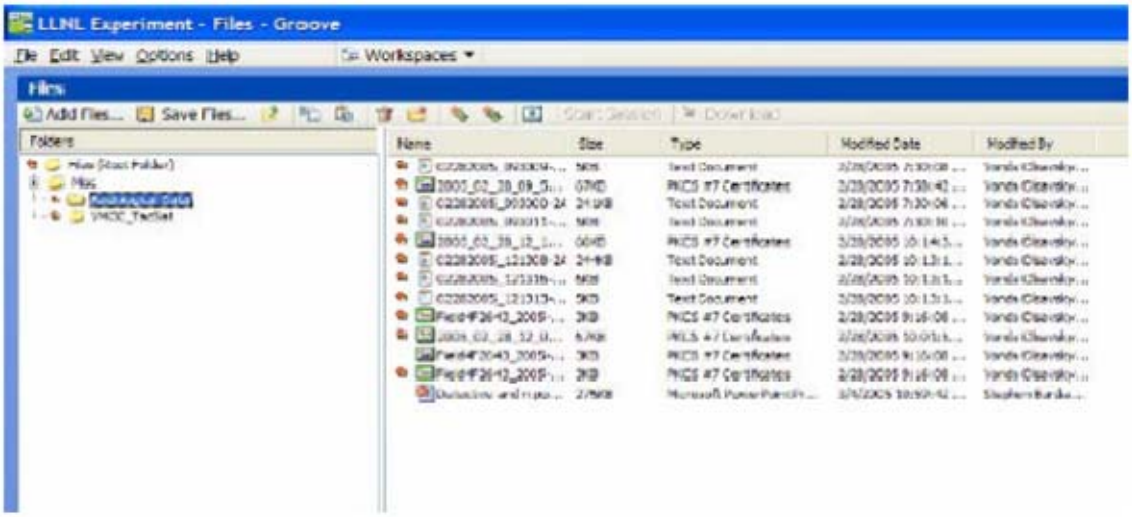

Figure 2. Snapshot of Radiological Files Posted in LLNL Workspace (From TNT 05-2 AAR)

- Pictures- to display or share photos or graphics
- Chat- to chat within workspace
- Alerts- used to alert member's in a workspace when any changes have occurred
- Team formation- used to invite members into a workspace through e-mail invitation or a file invitation
- Presence Awareness- allows workspace members to find out who is logged into Groove and in what subdivision of the workspace they are working
- Security- implements 192-bit encryption technology, which are Federal Information Processing Standard (FIPS) 140-2 and Common Criteria Evaluation Assurance Level (EAL) 2+ certified

For further information about this software, read NPS Thesis by Klopson and Burdian, March 2005 or www.groove.net.

2. SA Multi-Agent

The NPS SA Multi-Agent architecture was created in 2002 by Dr. Alex Bordetsky and Eugene Bourakov. (Bordetsky, 2002). The software development and implementation of SA Multi-Agent system is provided by Eugene Bourakov. The NPS SA uses maps or charts of the operating area of interest. Three ways to plot agents on the map are by clicking and dragging a symbolic icon (i.e. person, vehicle, sensor, etc.), by entering a latitude and longitude associated with a symbolic icon, or by Global Positioning System (GPS) device. (Klopson & Burdian, 2005) Figure 3 below shows a "snapshot of OFDM throughput-distance relationship analysis experiment. In the figure, the balloon icon is used to represent the Man-Pack/LRV mobile OFDM node." (TNT 05-2 AAR) Furthermore, the following are its features, which help to enhance the shared updates:

- Real-time shared updates on icons to enhance the SA of the operation.
- Voice and/or visual alerts on updates to prompt users of any changes.
- Customizable background maps to enhance the SA of the environment.
- Replay capability available through database storage of historical changes.
- Instant Messaging available by composing a message and dragging to the recipient's icon.
- Agent Information Sharing is available through an "Info" arrow button dragged and dropped on the icon representing the agent of interest. This method allows the user to view network connection status, general agent information, and to hear or see the agent (if this capability is set up). Video and audio triggers can be enabled or disabled to either transmit or not when there is any motion or sound detected at the location of the agent of interest.
- The Alert System provides alerts which are agent generated to notify other active agents of the alert being posted. Active agents then drag and click the "Info" arrow above the alert for amplifying information.

For further information about this software, read the NPS thesis by Klopson and Burdian, March 2005.

3. EWALL

EWall is an application which is used to help users to have situation awareness through the use of five Modules, which are aimed at "making administering, monitoring, collecting, exchanging, and visualizing information more intuitive. These modules support the manual, semi-automatic, and automatic creation of EWall Cards as well as the search, exchange, and organization of EWall cards, which are visual representations of files, much like desktop icons." (EWALL Introduction, 2008) EWall can help decision makers in a MIO environment to handle the abundance of information flowing into their station. The individual EWall cards appear on its workspace as shortcuts

organized with the rest of the cards in the order of sequence on a timeline. Organizing the files retrieved from various remote or local nodes in a MIO network is essential to expeditious MIOs, which results in a greater advantage against terrorists in the time domain.

4. NPS Video Conferencing (VC)

Video conferencing is a collaborative tool in which a camera and voice equipment is used to enhance the data-sharing relationship between various local and remote nodes. By looking and hearing each other through VC, the decision-makers can make decisions based on first-hand information without the risk of misinterpretation or time delays. When data sharing has to be done without the process of downloading, posting, or retrieving, VC allows the participating nodes to collaborate information in a real-time manner, thus allowing for a quick turn around for further investigation or actions. For the decision-makers, this tool allows them to quickly receive important updates or send life saving orders. NPS VC allows the users in a portal to communicate via chat, voice, video, or data file transfers, thus allowing the users various ways to share data expeditiously.

5. Observer's Notepad

This tool allows the participants, especially those located at the TOC or NOC, to post observations with time stamps throughout the operation. These notepads are organized by dates and chapters in order to quickly retrieve information in an organized manner.

6. Cellular Phones

Cellular phones are very popular in today's society to communicate near real-time information. This is why cell phones have become an excellent back up to other standard military communication tools. The only drawback to cell phones is that it does not provide the security needed, when there is sensitive classified information that needs to

be shared. Furthermore, use of cell phones is limited to areas where there is a coverage area by one of the various cell phone companies' networks.

7. Kockums Blue Force Tracker (BFT)

BFT is a C2/tracking-system constructed of off-the-shelf hardware and presented in a GIS. It's a peer-based design where all thorough units are equal members and no node is critical in the network. Nodes are connected Ad-hoc to the network and the system will automatically choose the best availably transmission (Automatic routing). Every node is equipped with a laptop, GPS, and a communication path to the network. (TNT 07-4 AAR)

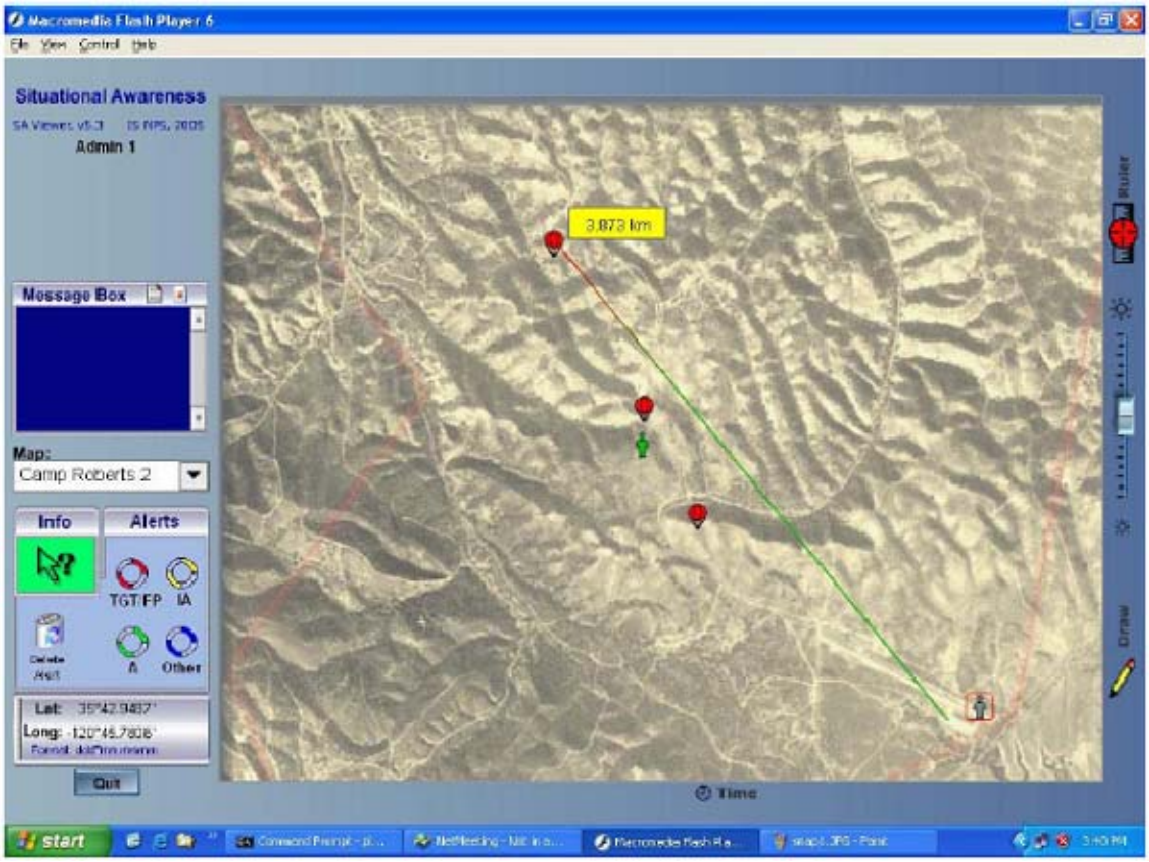

Figure 3. Snapshot using SA Multi-Agent System
(From TNT 05-2 AAR)

C. REQUIRED DATA TO ENHANCE SA AND DM

1. Nuclear Radiation Data

Nuclear radiation data can be captured through sensors developed either by the LLNL or IST, which have been tested during EMIOs. This data can be used to evaluate an alert from a BP, which has interdicted a suspected HVT and would like to know whether or not to detain the vessel and its crew or allow it to continue. Normally, the BP has radiation detection sensors, like the ARAM or IdentiFINDER, which can be triggered by anything as small as an old smoke detector or decaying food. It is necessary to quickly provide the detected radiation data to remote experts, which can analyze it and disseminate accurate reports back to the TOC, which can make the decision of whether or not to continue the search of the source of radiation or to continue with another task on board the TV.

2. Biometric Data

Biometric data can be captured through BFC's biometric devices and sent as files through the network to the BFC. These files can then be analyzed and matched with suspects on a pre-established database or watch list. Furthermore, with the collaboration of other agencies, like the FBI, International Police, or foreign agencies, these analyzed files can further enhance the usefulness of this method of suspect identification. Currently, the biometric data that has been used in MIO experiments have focused on digital fingerprints. The BFC is looking into incorporating facial recognition among other biometric identification methods.

3. Video

Video allows the C2 element to participate in the boarding. When a TOC commander sees something that he/she can relate to some past experience or knowledge, that commander's decision to act on that knowledge or experience can help the boarding officer in performing his duties. For instance, if the commander believes that the radiation source is possibly hidden behind a panel on the bulkhead which he/she can see

through the streaming video, he/she may take into account a past experience or knowledge about a possible explosive trap that might be triggered upon the removal of the panel. Furthermore, the video can also assist in legal matters when a crew decides to resist boarding for inspection and takes hostile action towards the boarding crew, which then results in commensurate force to apprehend the crew. The idea behind video streaming can benefit any participating node that must see what's going on in order to actively participate without becoming a hindrance in the decision-making process. Therefore, it may not be necessary for everyone to have access to the video.

4. Chat or Instant Messaging

The communications between the BP and the boarding vessel or TOC is necessary in order to provide information about the mission or any updates. Although, video and voice conferencing are great methods of achieving this, those methods can go down intermittently from data congestion in the network. Chat and Instant Messaging (IM) are reliable forms of communicating the situation and providing guidance on decisions made about the captured or processed data. Furthermore, Chat or IM can provide a legal record or a playback capability to find out what happened at a particular step of the boarding.

5. Voice

Although voice communications have been used often to communicate between two parties, it has been done using various methods, like handheld radios, cellular phones, or VoIP. In order to corroborate data by speaking to the Boarding Officer or a BP member with other remote participants, it must travel via VoIP in order to give everyone an opportunity to hear what is happening. Voice is a near real-time method of enhancing SA and decision-making process or actions. Furthermore, it gives the TOC quick access to the Boarding Officer's cognitive domain by stepping in to guide certain steps of the boarding process.

6. Files

The best way to involve remote experts or facilities not involved in a MIO network or workspace is to be able to send them a file of pertinent data of what the Boarding Officer or TOC wants processed. It could be a file containing scanned paperwork or documents, scanned/digital pictures, files captured from the crew's computer, etc. The importance of sharing files and updating any information related to them is essential in MIO collaboration. File sharing and updates can be enhanced with the use of collaborative tools in which those participants involved can receive the files and alerts on any updates to those files.

D. ENSURING THE DATA'S CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

These MIO experiments utilized a large number of Virtual Private Network (VPN) tunnels to connect sites across the country and around the world, in order to provide reliable and secure real-time information sharing. All VPN tunnels were configured across the open Internet, leveraging commercial wired and satellite services to physically connect sites. The VPN infrastructure used to support this experiment consisted of both enterprise- and SOHO-level equipment, including CISCO and Netgear brand services.

The configuration used in this experiment placed the Naval Postgraduate School at the center of a hub-and-spoke architecture, with all other sites connecting to a central VPN concentrator. In addition to the remote networks connected via LAN-to-LAN tunnels. Many remote participants, including those from Lawrence Livermore National Labs, connected via software VPN clients. The VPN infrastructure was also extended across a commercial satellite link into the Riverine operating area inside San Francisco Bay, further stretching into the tactical last-mile solution space. (TNT 07-4 AAR, 10)

The VPN concept was created to allow distributed users to use the public internet without the frustration of dealing with costly security measures that can deflect a budget better dedicated to other resources. VPN's features help to deflect hacker attacks like eavesdropping, masquerading and man-in-the-middle. (Farrell, 2006) By encrypting and

authenticating both ends of a VPN connection, users can share data without the frustration that confidentiality, integrity and, availability of the data has been delayed, compromised, or tampered.

III. SUMMARY ANALYSIS OF THE DATA SHARING ENVIRONMENT IN PREVIOUS MIO EXPERIMENTS

The network of data-sharing from the beginning of MIO Operational Experiments has grown from just a few nodes within the Monterrey Peninsula in California and two remote nodes, LLNL and NRL TACSAT, to world wide collaboration from countries like Sweden, Austria, and Singapore. As shown in the figure below, the MIO data sharing network continues to expand to involve more geographically distributes nodes.

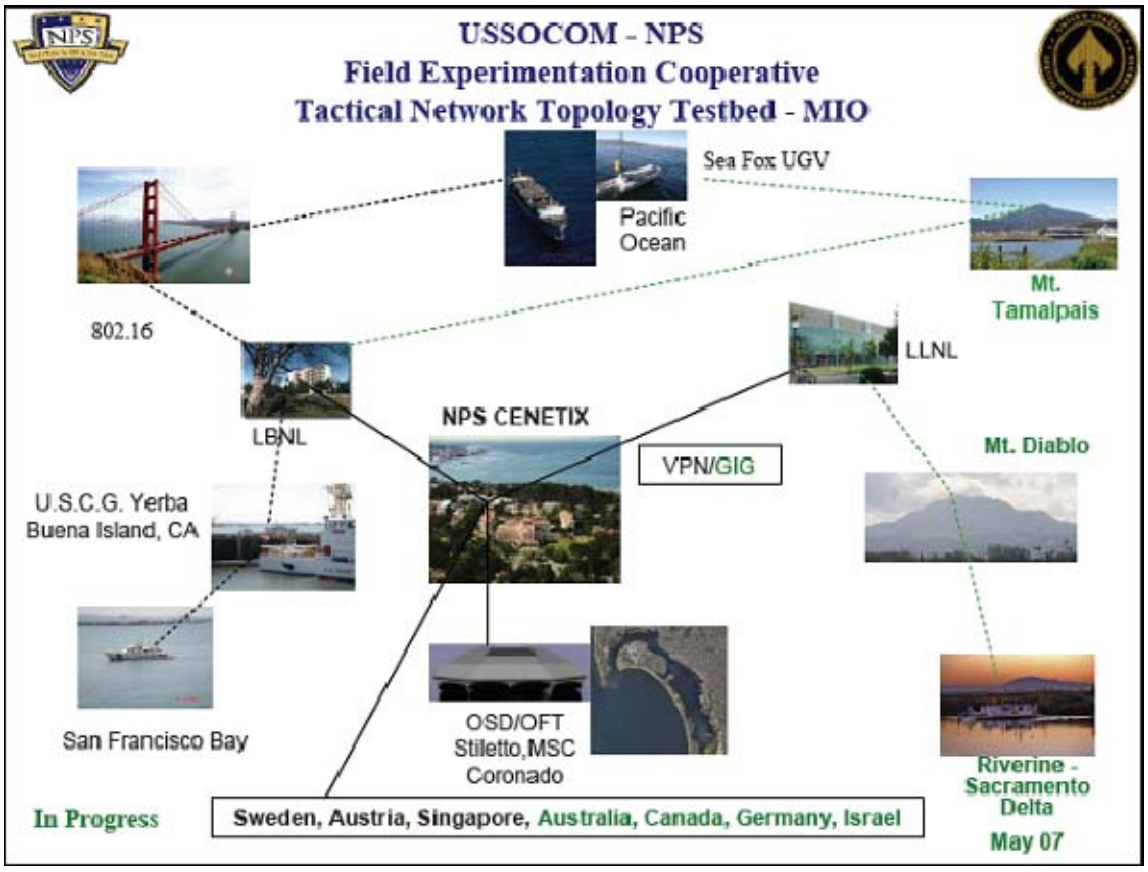

Figure 4. MIO Collaboration from Distributed Nodes
(From Bordetsky & Friman, 2007)

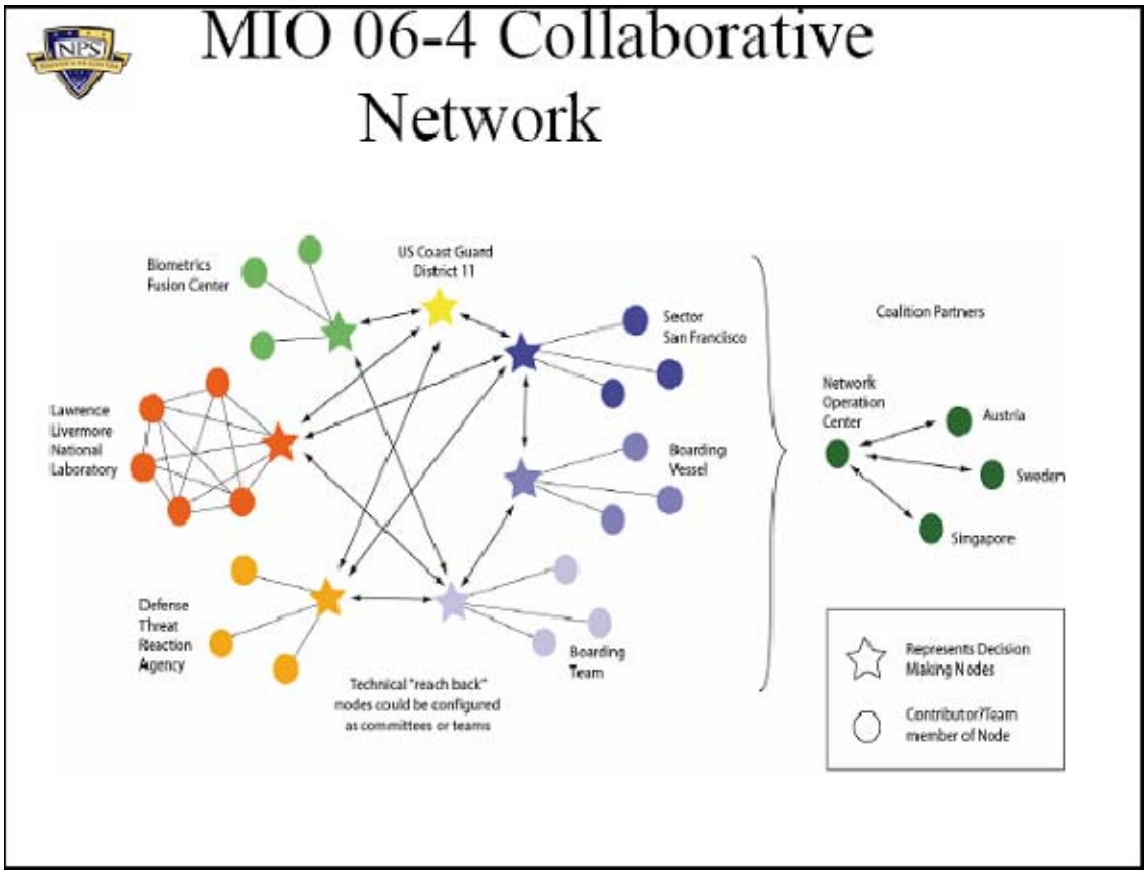

Figure 5. Distributed Node Collaboration to Support DM Nodes During MIO's (From Bordetsky & Friman, 2007)

The following information on previous MIO experiments was summarized from After Action Reports (AAR) and NPS Theses from Marvin, Klopson, Burdian, and Stavroulakis. The information about the network technology and sensors used serve to understand the environment and network infrastructure upon which the collaborative tools rely to provide data sharing to participating nodes. The figure above shows what the collaborative network should be able to do for the decision makers. Results about the data sharing with collaborative tools and the network infrastructure are also included in the following summary reports.

A. TNT MIO 05-2

During this experiment, held in Monterey Bay, the following information and results were recognized.

- Network Technology:
  - 802.11b for Mesh Network between Hawksbill and Cypress Sea
  - 802.16 (WiMAX)/OFDM between Cypress Sea and Beach Station, between Beach Station and NPS Spanagel Tower, between Spanagel and NPS Root Hall (NOC)
  - Ethernet used to connect NPS NOC, TACSAT, and LLNL to internet.
- Radiation Sensors:
  - Rad Pager (gamma & neutron radiation)
  - IdentiFINDER (Radiation Isotope)
  - Neutron Pod (Helium-3 Detector)
  - Ortec Device (NORM, Medical, Industrial, Nuclear, and Natural Isotope detector)
- Collaborative Tools used to provide remote experts the capability to participate in the boarding.
  - Groove
    - NOC, the Cutter, the Boarding Team (BT), TACSAT, and the LLNL (to allow for information and file sharing and whiteboard functionality)

- NPS Situational Awareness (SA) Multi Agent System
    - NOC, the Cutter, the Boarding Team, TACSAT, and the LLNL (to view the position of all the others, receive real-time video from each other, as well as conduct real-time chat as required.)
- NPS VC1

- Results:
    - Communications established with all participants except Hawksbill using GROOVE due to intermittent connectivity problems with the 802.11 link between Hawksbill and Cypress Sea.
    - Video and audio established with all participants except Hawksbill using SA Multi Agent System.
    - TACSAT placed radiation Alert on SA screen. NPS NOC and Cypress Sea acknowledged.
    - TACSAT posted ELINT information and imagery files of Monterey Bay in Groove's LLNL Experiment Workspace.
    - Information on LLNL Groove Workspace was copied and placed in NOC Groove Workspace for synchronization with Cypress Sea.
    - BT did not have success transmitting downloaded radiation data from Rad Pager, IdentiFINDER, Ortec Device, and Neutron Pod from BP's laptop to Cypress Sea via 802.11 mesh network.
    - BP had success transmitting downloaded radiation data from Cypress Sea to NOC via 802.16/ OFDM network.
    - LLNL positively identified radioactive substance, once radiation files posted in LLNL workspace and alerts (via Groove messaging) acknowledge by LLNL and TACSAT.
    - The DNOC (Cypress Sea) shared NOC (NPS) Workspace.

- DNOC and Boarding Team (BT) shared same workspace when connected.
- NOC relied on DNOC as relay for the BT's information.
- DNOC was able to access LLNL Groove Workspace, if needed.

- Conclusions:
  - SA Multi Agent System provided each player with a common operating picture that actually depicted real-time locations and communications between all of the experiment's participants.
  - GROOVE Virtual Office allowed for improved synchronization of the data collected at sea to the NOC and scientists back at the lab for analysis.
  - The Groove collaborative application software saves all the text messaging that goes on between the participants, therefore, participants are able to go back to the Groove workspace and see the entire conversation that took place between them. Furthermore, all files that are saved in the workspace remain there (with a timestamp) until deleted.
  - The 802.11 link is susceptible to disruptions caused by various interferences such as cordless phones, Bluetooth devices, and microwave ovens, which are all used onboard Coast Guard Cutters and target vessels. Therefore, 802.16 should replace 802.11 in conditions similar to this in order to avoid connectivity problems which may inhibit, corrupt, or disrupt data-sharing with collaborating participants.
  - Groove provides an excellent system for secure file transfer, whiteboard, chat and other beneficial collaborative tools.

- SA Agent provides real-time video and position information of assets and targets to greatly enhance overall situational awareness of users.
- Both Groove and SA Agent can be used simultaneously to create an excellent Common Operating Picture (COP) for maritime and shore based Operation Centers, therefore meeting or exceeding expectations.

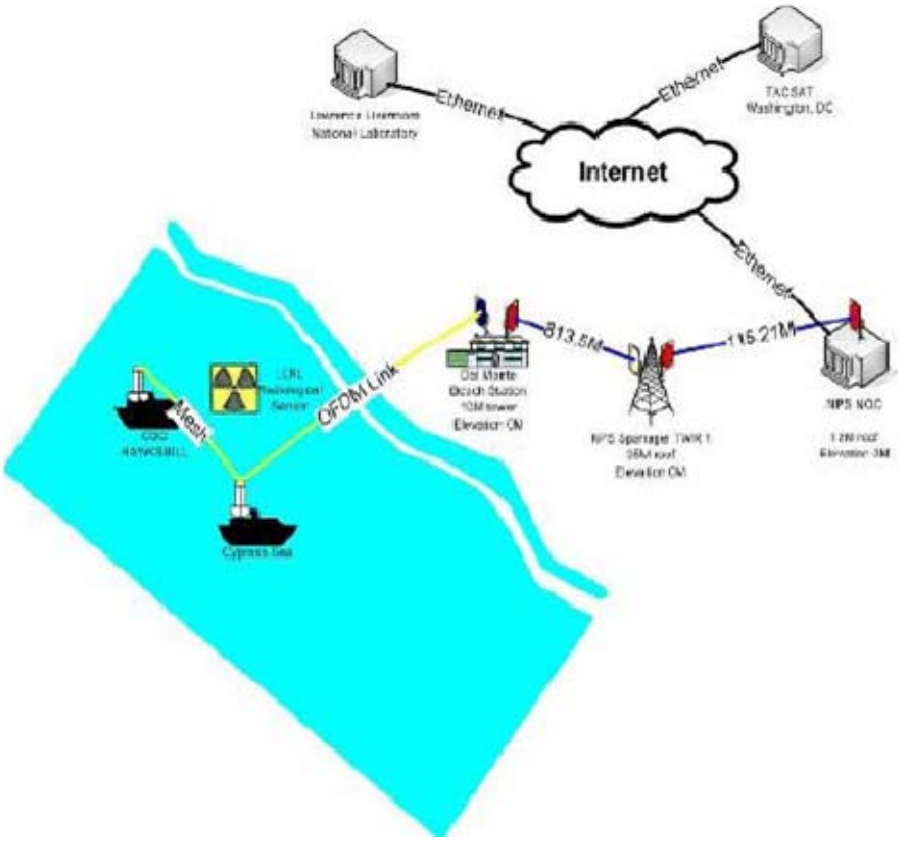

Figure 6. Network Configuration for TNT MIO 05-2
(From TNT 05-2 AAR)

Figure 7. Real-time SA Display in NOC, with Live Video from Cypress Sea (From TNT 05-2 AAR)

B. TNT MIO 05-3

This experiment, also held in Monterey Bay, provided the opportunity to test a simulated portable AN-50M from the target vessel to the Boarding Vessel (BV) and also test LLNL's UWB technology to transmit radiation data within the ship's structure. The following information and results were recognized.

- Network Technology:
  - 802.16/OFDM network between Hawksbill and Cypress Sea
  - 802.16 (WiMAX)/OFDM between Cypress Sea and Beach Station, between Beach Station and NPS Spanagel Tower, between Spanagel and NPS Root Hall (NOC)
  - Ethernet used to connect NPS NOC, TACSAT, and LLNL to internet.

    - UWB used to send radiation data from inside the ship's structure to an Ethernet switch connecting it to the Boarding Officer's laptop, hence the 802.16 link back to the Cypress Sea.

- Radiation Sensors:
    - GN-5 (from Innovative Survivability Technologies (IST))
- Collaborative Tools used to provide remote experts the capability to participate in the boarding.
    - Groove
    - Situational Awareness (SA) Multi Agent System
    - NPS VC1
- Results:
    - LLNL used a radiation material histogram to download into LLNL laptop and post to GROOVE workspace.
    - 802.16/OFDM had excellent throughput at extended range of 1,000 meters combined with low latency and resistance to interference.
- Conclusions:
    - 802.16 should replace 802.11 to maintain or to enhance data sharing in long range conditions, or conditions with signal interference, such as strong Electromagnetic Interference (EMI) or Radio Frequency Interference (RFI) from shipboard or personal electronic or electrical equipment.

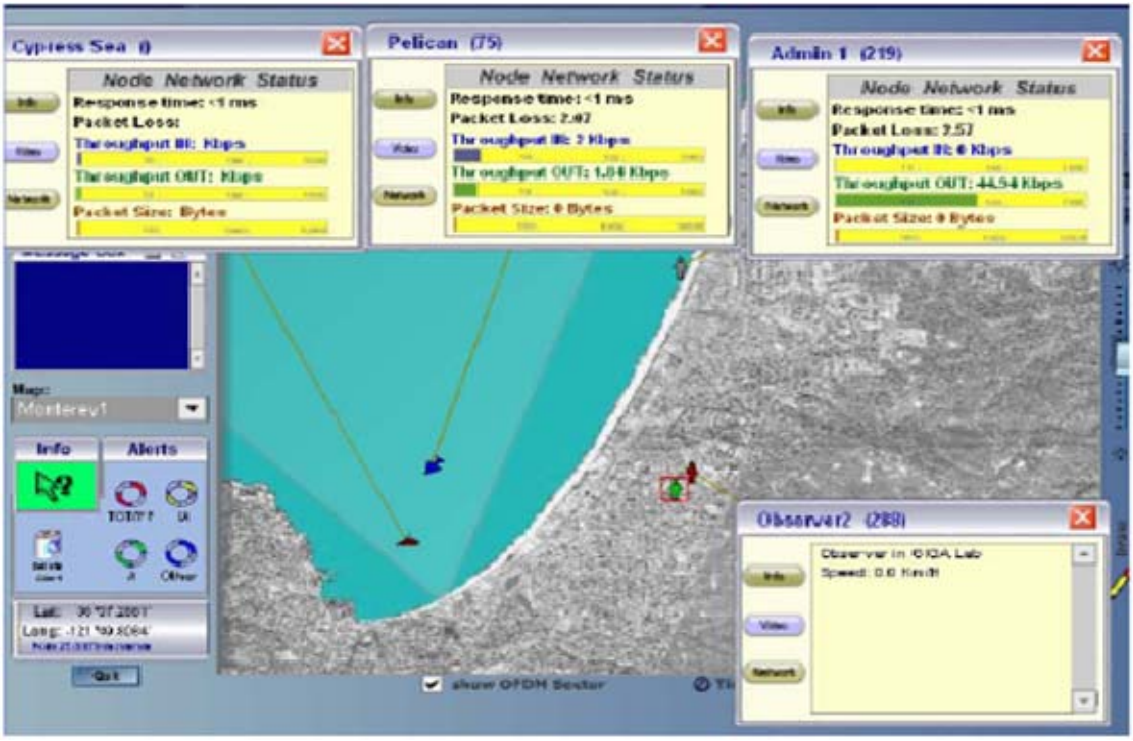

Figure 8. SA Assets in Monterey Bay
(From TNT 05-3 Full AAR)

C. TNT MIO 05-4

This experiment provided the opportunity to test the AN-50M (portable 802.16/OFDM) at a longer range of 2,000 yards and the GN-5 radiation detector. LLNL's UWB technology was re-tested by transmitting radiation data from the downloaded radiation files from IST's GN-5 radiation detector. The following information and results were recognized.

- Network Technology:
  - AN-50M link between Hawksbill and Del Monte Beach Lab
  - 802.16 (WiMAX)/OFDM between Beach Station and NPS Spanagel Tower, between Spanagel and NPS Root Hall (NOC)

- Ethernet used to connect NPS NOC, TACSAT, and LLNL to internet.
- UWB to send radiation data from inside the ship's structure to an Ethernet switch connecting it to the Boarding Officer's laptop, hence the 802.16 link back to shore.

- Sensors:
  - GN-5 (from IST)
  - Fingerprint Reader (from BFC)
- Collaborative Tools used to provide the remote experts the capability to participate in the boarding.
  - Groove
  - NPS SA Multi-Agent System
  - NPS VC1
- Results:
  - LLNL able to download radiation material data from GN-5 to post on GROOVE workspace.
  - AN-50M had excellent throughput of 1.0 Mbps at extended range of 2,000 yards. Foliage near the Del Monte Beach Lab was a probable contributing factor to a decreased data rate.
  - GROOVE facilitated voice and chat.
  - LLNL and BFC were able to open GROOVE files in less than two minutes.
  - Biometrics data collection and processing of 5 "ten print" cards took 15 to 20 minutes.
  - Operational coordination was handled by VoIP to various nodes.
  - Group Chat and Text Messaging was also used extensively.

- SA Multi Agent worked well to provide limited positional data and alerts to large events.
- Video Conference was a problem via ISGIANT/VC1 server at NPS.

- Conclusions:
  - The use of the 802.16 link through the portable AN-50M continues to prove its reliability, even at longer ranges to enhance data sharing.
  - GROOVE and SA Agent continue to prove their reliability to provide a usable workspace and to enhance SA for remote nodes.
  - VC1 can continue to be a useful tool if the server problems are resolved.

D. TNT MIO 06-1

This experiment, conducted in Alameda, California, was an opportunity to continue rapidly deployment evaluation of networks and advanced sensors in MIOs. To simulate the operational conditions of a realistic MIO, it was essential to focus the efforts of this experiment in the BP's ability to rapidly set-up ship-to-ship communications in order to search for radiation and explosive sources while keeping in contact with the BV and collaborating with remote sensor experts. The following facts were recognized.

- Network Technology:
  - Portable AN-50M (802.16/OFDM) link
  - 802.16 (WiMAX)/OFDM
  - Ethernet used to connect NPS NOC, TACSAT, and LLNL to internet.

- UWB to send radiation data from inside the ship's structure to an Ethernet switch connecting it to the Boarding Officer's laptop, hence the 802.16 link back to shore.

- Sensors:
  - GN-5 (from IST)
- Collaborative Tools used to provide remote experts the capability to participate in the boarding.
  - Groove
  - SA Multi-Agent
  - NPS VC1
- Results:
  - LLNL able to download radiation material data from GN-5 radiation detector to post on GROOVE workspace.
  - AN-50M had excellent throughput of 1.0 Mbps at extended range of 2,000 yards. Foliage near the Del Monte Beach Lab was a probable contributing factor to a decreased data rate.
  - GROOVE facilitated voice and chat.
  - LLNL and BFC were able to open GROOVE files in less than two minutes.
  - Biometrics data collection and processing of 5 "ten print" cards took 15 to 20 minutes.
  - Operational coordination was handled by VoIP to various nodes.
  - Group Chat and Text Messaging was also used extensively.
  - SA Multi-Agent worked well to provide limited positional data and alerts to large events.

- The use of 802.16 technologies through the portable AN-50M continues to prove its reliability, even at longer ranges to enhance data sharing. An autonomous, advanced ship-to-ship communication capability and network during simulated MIO within 15 minutes was successfully established.
- Biometric and radiation detection data were successfully and accurately transmitted to the BFC and Lawrence Livermore National Laboratory.
- The VPN access to OFDM-ITT Mesh network disabled the Groove clients in several nodes. Precise configuration of every laptop stack resolved the problem.
- The Boarding Party was able to provide biometric data and Radiation Detection Data via VPN reach back to Biometric Fusion Center and LLNL.
- The response time for biometrics data sharing and response from the BFC was reduced to 4 min.
- Latency of sync with all sites (out band coordination): less than 2 min
- Robust Groove data sharing applications network between the Boarding Party Members and remote experts permitted the team to make decisions to proceed to the next step in the process in a period of 2-4 minutes; e.g. from biometrics ID (BFC) step to the search for non-proliferation machinery (DTRA) step, etc.

- Conclusions:
  - GROOVE continues to prove its reliability to provide a usable workspace for remote nodes.
  - Man-Pack OFDM network combined with ITT mesh along the deck is feasible.

- Ultra-wide-band (UWB) link from the top deck to two floors down to the radiation and explosive detection sensors also appeared to be feasible.
- ITT mesh connectivity is vulnerable to obstacles.
- Streamlining VPN with mesh routing is essential for future operations.
- Video Conference continued to be a problem via ISGIANT/VC1 server at NPS, but can prove to be a valuable tool.

E. TNT MIO 06-2

This MIO experiment was held, once again, in Alameda, California. It provided the opportunity to test the FLASH/OFDM Wireless PC card which falls under the 802.20 wireless technologies. The following information and results were recognized.

- Network Technology:
  - 802.16/OFDM network between SS Gem State and USCGC Tern
  - 802.16 (WiMAX)/OFDM between Cypress Sea and Beach Station, between Beach Station and NPS Spanagel Tower, between Spanagel and NPS Root Hall (NOC)
  - Flash/OFDM 802.20
  - Ethernet used to connect NPS NOC, TACSAT, and LLNL to internet.
  - UWB to send radiation data from inside the ship's structure to an Ethernet switch connecting it to the Boarding Officer's laptop, hence the 802.16 link back to the TOC.
  - ITT Mesh network to send streaming video from BP's RHIB back to BV

- Sensors:
    - Biometrics Station with Fingerprint Reader
- Collaborative Tools used to provide remote experts the capability to participate in the boarding.
    - Groove
    - NPS SA Multi-Agent System
    - NPS VC1
- Results:
    - VPN provided real-time shared access of operational events (UAV video, photos, BFC data) allowing BFC, USSOCOM and USCG Alameda to participate.
    - Multiple Human System Integration (HIS) issues within the TOC were identified:
        - TOC command area should be restructured to emphasize personnel placement according to area of responsibility
        - Routine confusion among TOC personnel noted because of inadequate data screen labeling or screen prioritization
        - Frequently redundant data windows displayed
    - During BP's transit via RHIB to TV (USCG Tern) adequate streaming video was received in VC1 through the ITT mesh, as long as there was clear LOS, which was achieved up to a maximum range of 500 yards.
    - 802.20 had outstanding performance maintaining connection at "near" Line of Sight (NLOS) conditions.

- 802.16 had connectivity issues unless LOS was obtained through manual antenna alignment. Self-aligning antennas will solve this problem.
- Ship's navigation radar and 802.20 do not affect the 802.16 link connectivity.
- Radiation and biometric data files were sent to remote experts at average distance of 1,000 yards via 802.16.
- 802.16 maintained connectivity at a maximum distance of 2,000-2,400 yards.
- NAT router settings at USCG Alameda inhibited NPS NOC from receiving or monitoring data remotely.
- Lack of GPS devices connected to BO's and BFC's laptops resulted in no data capture of time or position of both laptops.

- Conclusions:
  - 802.16 and 802.20 links working together to transmit data helped to maintain or to enhance data sharing.
  - 802.20 performed well up to a distance of 3 nm from the base station and NLOS conditions.
  - UWB wireless LAN performed well, providing radiation material pictures and video from internal spaces to be transmitted to the TOC.
  - ITT Mesh network performed well, allowing streaming video from BO's laptop to reach the TOC onboard the BV (Gem State) at a distance of 500 yards.
  - Groove provided the collaboration workspace to enhance the BO's SA in order to take the right steps based upon the decisions made by remote participants/experts.

F. TNT MIO 06-3

During TNT 06-3, more participants were added to the collaboration environment to better evaluate the situational awareness and correct decision-making process during a more complex scenario.

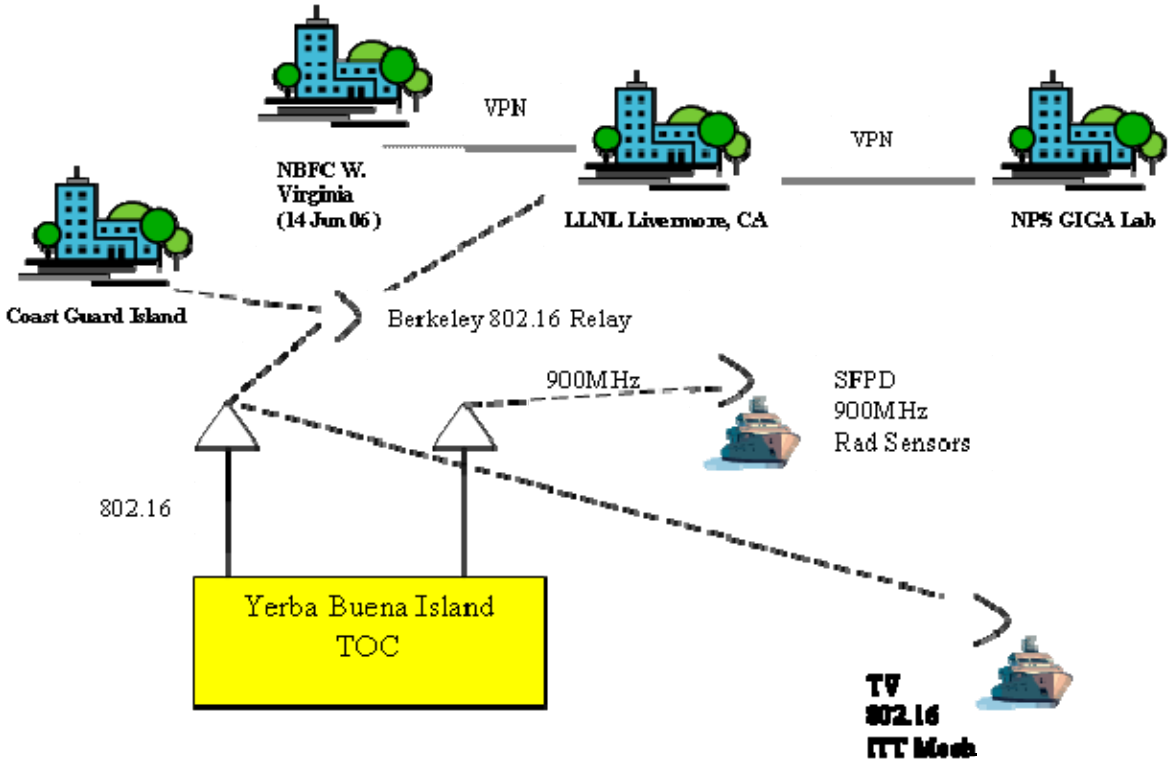

Figure 9. TNT 06-3 MIO Experiment Network Overview
(From TNT MIO 06-3 AAR)

- Network technology
    - 900 MHz link to connect YBI TOC to SFPD Marine Unit-3 RHIB
    - ITT Mesh to connect YBI TOC to TV. The internal ITT mesh included Solar Winds monitoring laptop and ITT Mesh access point with local GPS receiver.
    - ITT Mesh between BO's network monitoring laptop and ITT AP with Garmin GPS receiver and poster
    - 802.16 from TV (Alameda County Sheriff Marine Patrol Boat) to YBI TOC, from YBI TOC to Alameda Island, from Alameda to LBNL, from LBNL to USCG Island to access public internet through VPN tunnel back to the TNT network
- Sensors
    - IdentiFINDERS from LLNL
    - Biometric Fingerprint Device
- Collaborative Tools
    - Groove participants
    - NPS SA Multi-Agent System
    - NPS VC1
    - E-Wall data fusion and situational awareness memory mechanism
- Results
    - Live collaboration and decision-making (voice, video, and data) successfully utilized to conduct boarding and search with inputs from Sweden and Austria.
    - Three sets of fingerprints were sent from Biometrics enrollment laptop to the Biometrics Master computer at the USCG YBI TOC.

- Obtained radiation files were transferred from IdentiFINDERS from MSST to LLNL laptop and from there to the BP's Groove laptop via flash memory stick to post to Groove Workspace because LLNL laptop was not loaded with Groove's client software.
- Incorrect time stamps on all Groove client laptops. CENETIX server GPS time sent to all Groove laptops to keep time stamps correct and consistent.
- Incorrect labeling of two posted radiation files on Groove caused confusion regarding the first radiation source detected by MSST.
- Photographs of radiation source #2 downloaded to BO's laptop and posted on Groove further help identify the source.
- The three following Groove Workspaces used incorrectly probably from complexity of environment:
    - District 11, for C2 and DM
    - BP
    - Network for technical and experiment issues
- Boarding Party replaced omni-directional antenna for the 802.16 link from TV to TOC to avoid having connectivity problems from lack of LOS.
- 802.16 link was stretched to only 700 yards, due to directional antennas being replaced with omni-directional ones with 6dB gain.
- Target Vessel's navigation radar (Furuno, I-band/9 GHz) did not affect the performance of the 802.16 or 900 MHz links.
- AN-80s could not be configured to be used on TV, although successful previously at Camp Roberts.

- The BO's network monitoring laptop and GPS receiver/poster laptop had negligible contribution to 802.16 total throughputs which was estimated at 2 Mbps.
- The Yerba Buena Island TOC was unsuccessful in establishing 802.16 connections with LLNL. Problem is suspected to be with LLNL configuration. Also, Yerba Buena Island TOC was unable to access Groove area, via Coast Guard Island. Possible cause is a bad relay server, which is required for the collaborative network, including files transfers for Biometric Fusion analysis and radiation spectrum analysis by LLNL.
- Several problems caused inability to establish solid Groove participation at TV. Server at Coast Guard Island was overloaded (connection to NPS server is through this server and 802.16 connections at TOC). Intermediate 802.16 link connectivity between TOC and Berkeley 802.16 relay, thus keeping LLNL out of Groove area, was eventually worked out.
- Successfully proved the 802.16 link connectivity between TV NOC and TOC through ability to view TOC roof camera on TV NOC laptop.
- Radiation information was transmitted, via Groove workspace, to LLNL Watch Office via 900MHz connection between SFPD boat and TOC.
- SFPD could not directly transfer spectrum file since complete software was not loaded onto their laptop.
- Boarding party successfully boarded TV and conducted search for 3 hidden radiation sources. Boarding party found all three sources and submitted 3 reports, via Groove workspace to District 11.

- During boarding, replaced 5-port switch with 8-port switch to allow room for Biometrics Enrollment laptop and additional Groove laptop.
- Biometrics personnel were also taking and submitting fingerprints to Biometrics Master Computer, located in TOC, via the 802.16 link between TV and TOC. Message was sent from BP to TOC via Groove that fingerprint files were available.
- MSST successfully found radiation source after boarding. Data was transferred via oral report to Boarding Officer (played by NPS personnel) and entered into Groove Workspace with LLNL Watch office. Boarding Officer also provided USCG District 11 regular status reports.
- MSST successfully found second radiation source and submitted information orally to Boarding Officer who entered information into Groove Workspace with LLNL Watch Officer. MSST later transferred spectrum data from first source to LLNL laptop which was then transferred to memory stick and then provided to Boarding Officer. Confusion arose due to mislabeling of source and noise on second set of spectrum data files. Once the files were correctly identified and posted to Groove Workspace, LLNL was able to review file and correctly determine that the source was Plutonium.
- Directly connecting digital camera to Target Vessel NOC laptop allowed BT to post picture of second radiation source (smoke detector) to Groove Workspace, which was reviewed and confirmed by LLNL to be a smoke detector.
- Conducted several successful radiation detection passes by SFPD boat and TV. Radiation information was transmitted, via Groove workspace, to LLNL Watch Office via 900MHz connection between SFPD boat and TOC.

- Conclusion
    - Overall, the 802.16 link had excellent performance and was able to accommodate the requirements of exchanged data.
    - There were no problems with the network reliability or performance.
    - Overall, the SA of all participants was sufficient to enhance the DM process.
    - The addition of international participants proved that there are no limits on who can be included and from where in the world.
    - TOC maintained connection with Berkeley relay, and thus LLNL via 802.16, and Coast Guard Island.
    - SFPD could not directly transfer spectrum file since complete software was not loaded onto their laptop.
    - Need to follow rules of Groove Workspace. Keep posting of files (radiation and biometrics) and message in Boarding Party workspace. Decision information should be kept in District 11 workspace. Network workspace should only be used for experiment control.
    - Need to configure laptop for Boarding Officer with proper Groove workspace.
    - Did get good video from Austrian source of vehicle. Still need to set up Groove Workspace for Austrians to use. Sweden also able to upload video/data via Groove in order to participate.
    - LLNL was able to open radiation file posted from TV NOC
    - Initially, SFPD used Groove to relay information to Radiological Assistance Program (RAP) personnel (via 900MHz connection to TOC). RAP will also get LLNL on Groove and USCG District 11.
    - Need to set time on all laptops to Internet time before starting experiments.

- MIO experiments accomplished what was required, set up network and used Groove Workspace to exchange information used for Boarding Party to make tactical decisions.
- Multiple Groove workspaces were confusing for LLNL and BP. Difficult to monitor all workspaces and update all required workspaces.
- LLNL needs PELCO software to view video through cameras on Target Vessel or TOC vice using photographs. It should be available to all participants.

Figure 10. TV Pre-Boarding NOC
(From TNT 06-3AAR)

G. TNT MIO 06-4

During this MIO experiment, the focus was to make the operational conditions more complex by adding more participants and sharing more data through them.

- Network Technology
    - Same as before. However, this was the first time Self Aligning OFDM (SAOFDM) antennas were used, providing 1.5- 3Mbps bandwidth support for collaborative tools and video feeds up to 4.5 miles off shore.
- Sensors
    - Same as before.
- Collaboration Tools
    - Same as before.
- Results
    - All CONUS and overseas nodes were able to interact in the collaborative environment with voice, data, and observe video and radiation detection from remote warning sites in Sweden, Austria, and Singapore.
    - Limiting visual detection was the hazy weather from fog and humidity.
    - Data sharing flowed seamlessly between participants, like the posting of video and radiation information by the Austrians to the sending and posting of pictures by the BP from the TV.
    - The NPS OFDM network successfully linked the ship and shore components in the San Francisco Bay area. It also linked the NPS NOC in Monterey to Camp Roberts, and the Stiletto to the Navy site ashore in San Diego. VPN connections linked the various

OFDM network components as well as the technical reach-back sites and the coalition participants.

- The network successfully linked all of the below players (see Figure 11) into the collaborative environment, including the Stiletto ship in San Diego acting as the Navy Cell and an adaptive networking node.
- Groove was used in the following ways to perform the following functions:
  - Discussion Board / Chat – for text communication between nodes. The discussion board is better than chat because it enforces hierarchy relationships of the different posts. This makes it much easier to follow information in the asynchronous and distributed decision making environment.
  - File Transfer – primarily for distributing data files from the BT to/from the Reach-back facilities.
- Task Manager – using this tool in the control (TOC and Networking) workspace gave participants an easy and informative way to monitor the progress of the scenario. It was an excellent use of a previously unused Groove tool.

- Conclusion
  - This experiment further evaluated the network and collaborative tools in a more realistic worldwide environment. The experiment further proved a successful network topology and collaborative tools supports a collaborative environment.
  - A solution to handling a complex MIO operational environment is to include more personnel at every level to manage data and technical issues.

- Everyone involved had near-real time, simultaneous access to the events as scripted and everyone was able to witness the events unfold at the same time.
- Overall, the situational awareness of all participants was sufficient to enhance the cognitive process and produce correct decisions, due to the participation of the right players in the collaboration environment and the use of Groove, SA and E-Wall collaboration tools.
- Once the network was established, data sharing was not an issue. However, network from mobile to stationary nodes had an impact on the quality and reliability of video between them. This was not a problem for fixed to fixed nodes. This is attributed to the LOS weakness of the 802.16 link.
- Duplicate information reported in multiple workspaces frequently interrupted the user's workflow. This can be solved by compartmentalizing personnel to specific workspaces and data.
- SA Agent provides the geographic positions of the assets and status of the network links for the mobile nodes.
- EWall was used to monitor information alerts. However, the sparse number of alerts posted in EWall limited the effectiveness of the tool during this experiment.
- VOIP phone was an excellent tool for voice communications. Video streams were monitored from various nodes, but this functionality was not critical to the D11 decision making process.

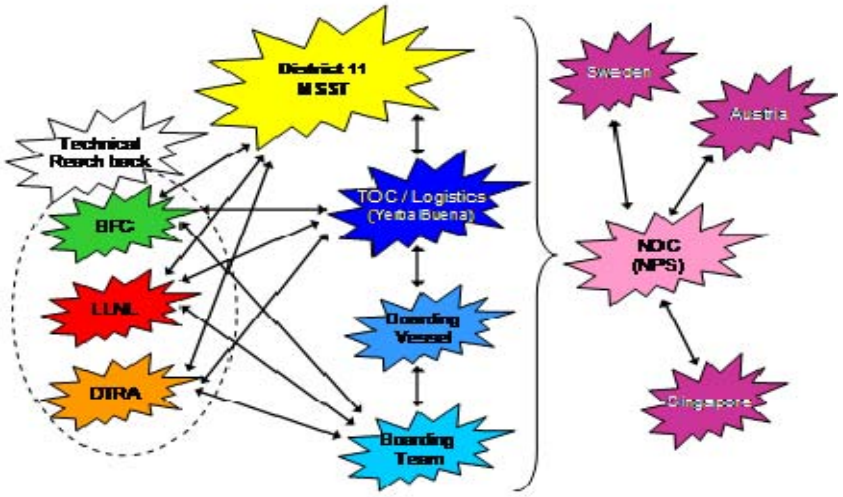

Figure 11. Collaborative Network

(From TNT MIO 06-4 AAR)

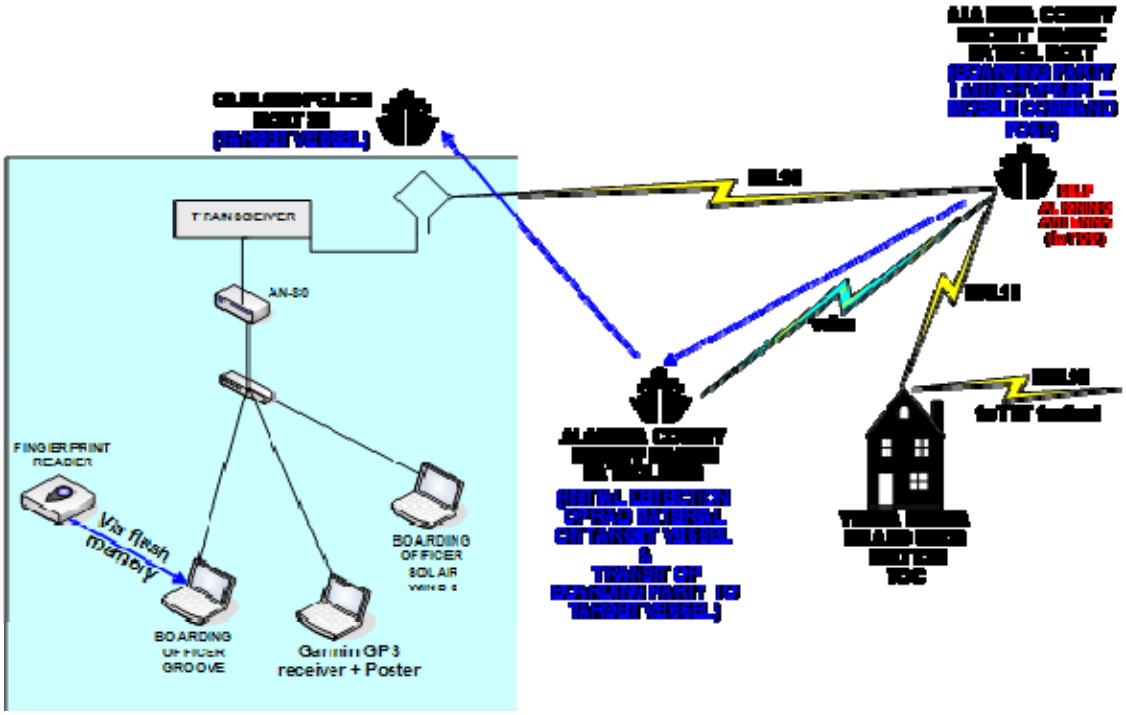

Figure 12. TNT 06-4 MIO Network in SF Bay Area

(From TNT 06-4 AAR)

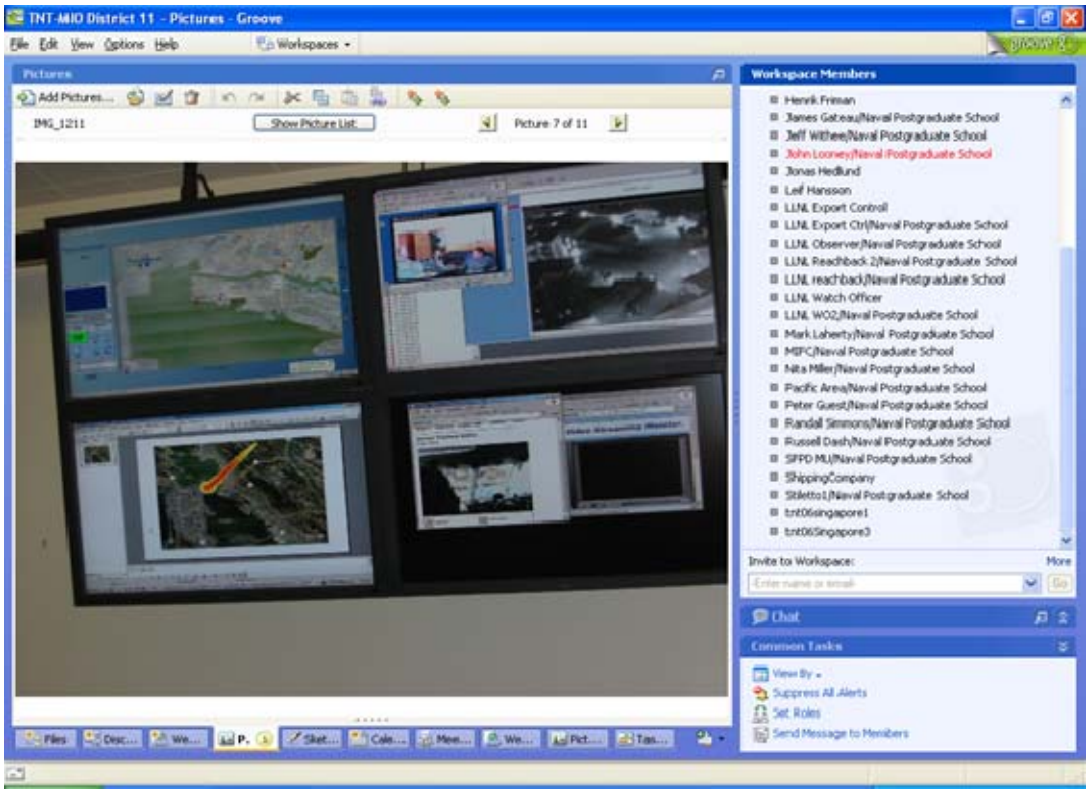

Figure 13. View of Groove Virtual Office used in San Diego
(From Bordetsky & Friman, 2007)

Figure 14. Streaming Video Teleconference Between Stiletto And CENETIX NOC
(From TNT 07-2 AAR)

H. TNT MIO 07-1

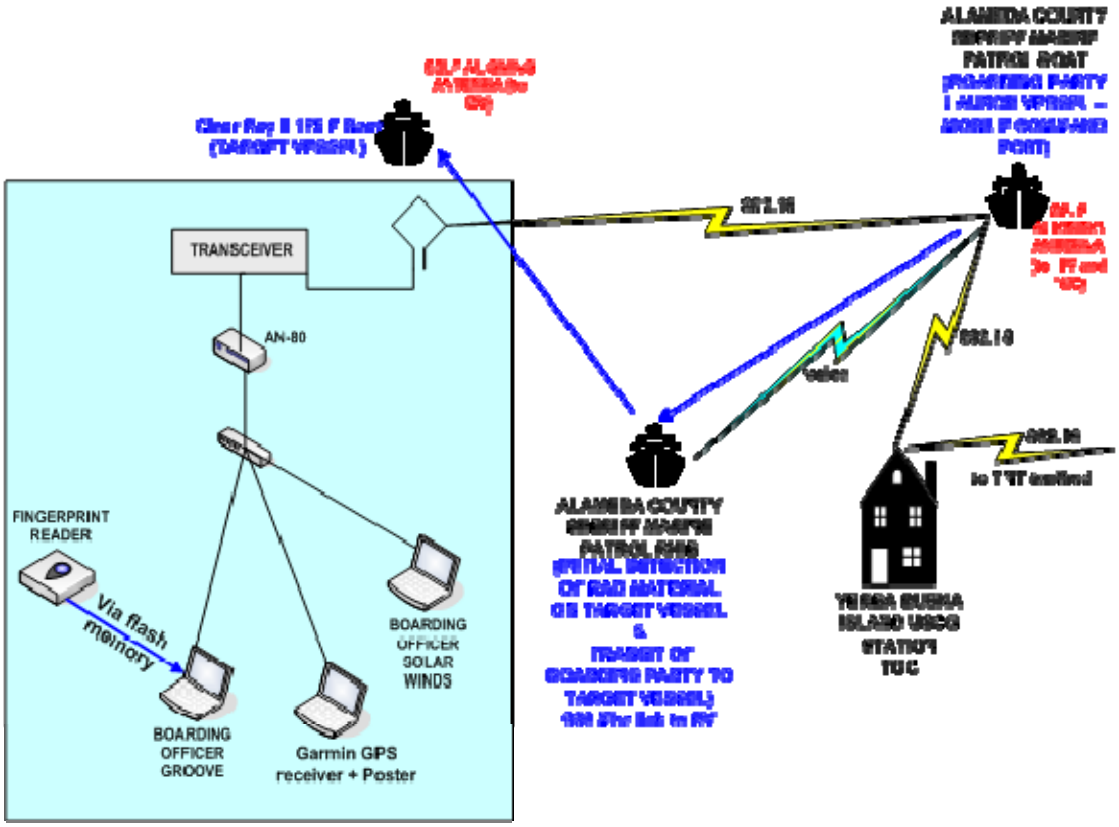

Figure 15. TNT 07-1 MIO Network in SF Bay Area
(From TNT 07-1 AAR)

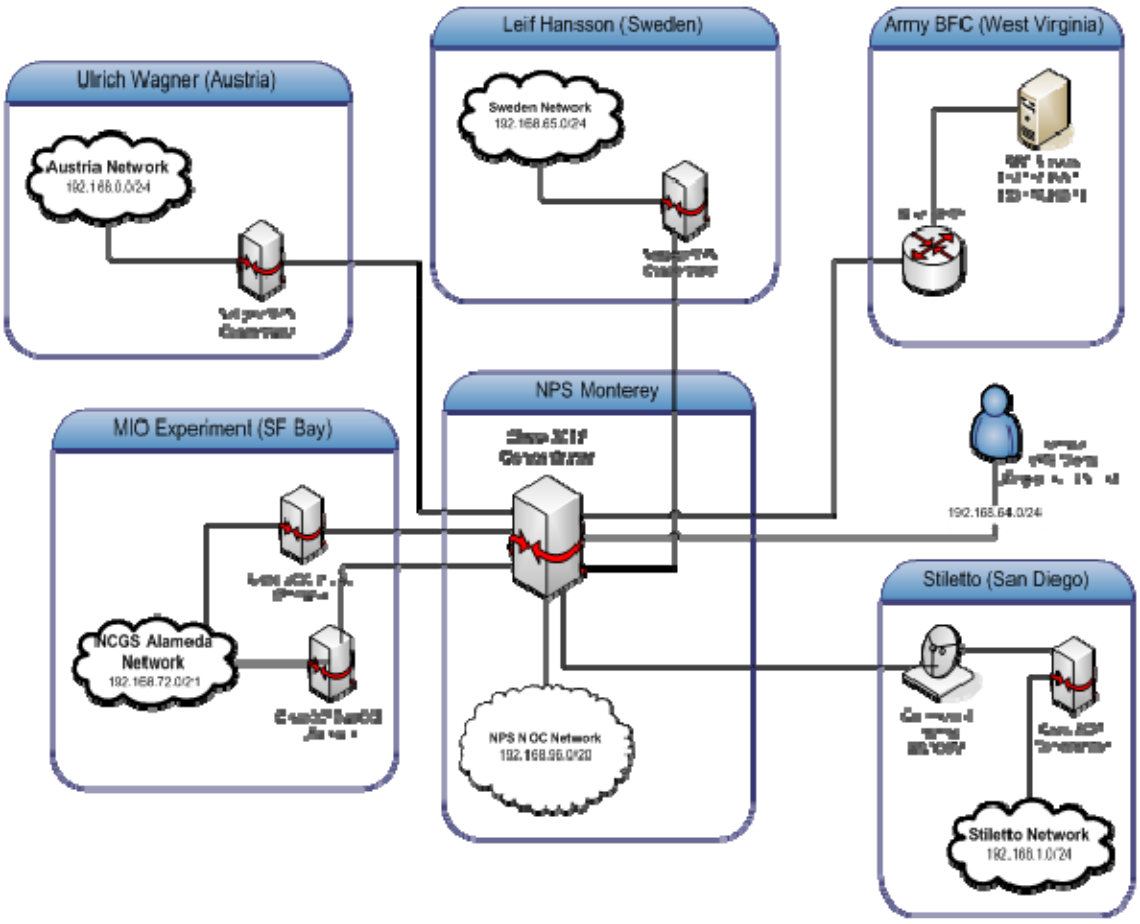

Figure 16. VPN Cloud Connecting MIO with Global Collaborators (From TNT 07-1 AAR)

Figure 17. SAOFDM Ship-to-Shore Link Operational on-the-Move in SF Bay (From TNT MIO 07-1 AAR)

Figure 18. Ship-to-Shore Link with BV behind Port Structures in the Channel (From TNT 07-1 AAR)

- Network technology
    - Self-Aligning OFDM (SAOFDM) 802.16 nodes for ship-to-ship and ship-to-shore wireless on-the-move networking.
    - Sky Pilot System and Radio over IP technology for Marine Corps DO Unit
    - Sea Fox Unmanned Surface Vehicle
- Sensors
    - USCG: IdentiFINDER (set to USCG specs), RadPager
    - SFPD: Sodium Iodide
    - IST: ARAM
    - LLNL: ARAM and IdentiFINDER
- Collaborative Tools
    - Groove peer-to-peer
    - NPS SA Multi-Agent System
    - NPS VC1
    - E-wall data fusion and situational awareness memory mechanism
- Results
    - Some of the challenges that were overcome involved the stability of the VPN infrastructure.
    - SAOFDM provided ship-to-shore communications with YBI TOC and between the boarding vessel and target vessel. However, it was still vulnerable to obstacles, which blocked its LOS path.
    - Sky Pilot broadband mesh network extended the MIO collaborative environment to a USMC unit conducting search for suspects in the port service area.

- The Sea Fox USV was used for the first time to target ship video observation ahead of manned operations.

- Conclusion
  - This MIO experiment continued to implement new technology to expand the MIO collaboration environment to geographically distributed participants.
  - The LLNL team achieved higher levels of performance in drive-by Radiation and Explosive detection combined with geographically distributed analysis. The overseas sites achieved more advanced level of multiple video feeds and collaboration and data sharing with MIO participants.
  - OFDM plus commercial satellite reach-back capability allowed the Stiletto ship in San Diego to participate remotely, providing real-time intelligence information into the scenario and conducting concurrent OFDM communication tests over water.
  - Swedish participants successfully connected to the experiment via the global VPN cloud (see Figures 16 & 19), and participated in video conferences as well as providing intelligence inputs throughout the scenario. The reach-back to Sweden was a simultaneous two-way exchange of two video streams concurrent with drive-by radiation detection data-sharing in Groove as seen in Figure 20, below.
  - The participants in Singapore also injected intelligence data during the scenario, and were successfully monitoring all video feeds during the experiment.
  - Managing VPN access lists continued to be an issue.

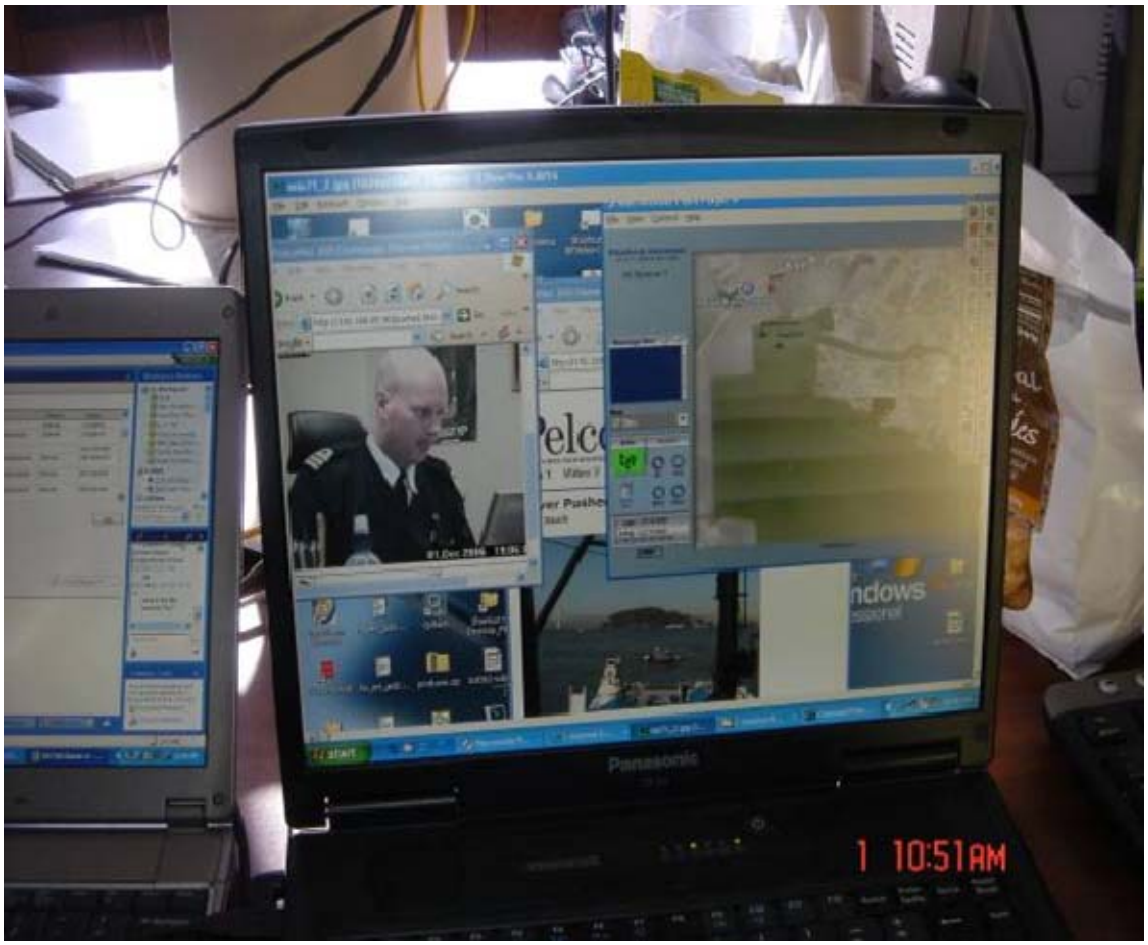

Figure 19. Swedish Collaborated Remotely Via VC1 and SA Interfaces (From TNT MIO 07-1 Final Report)

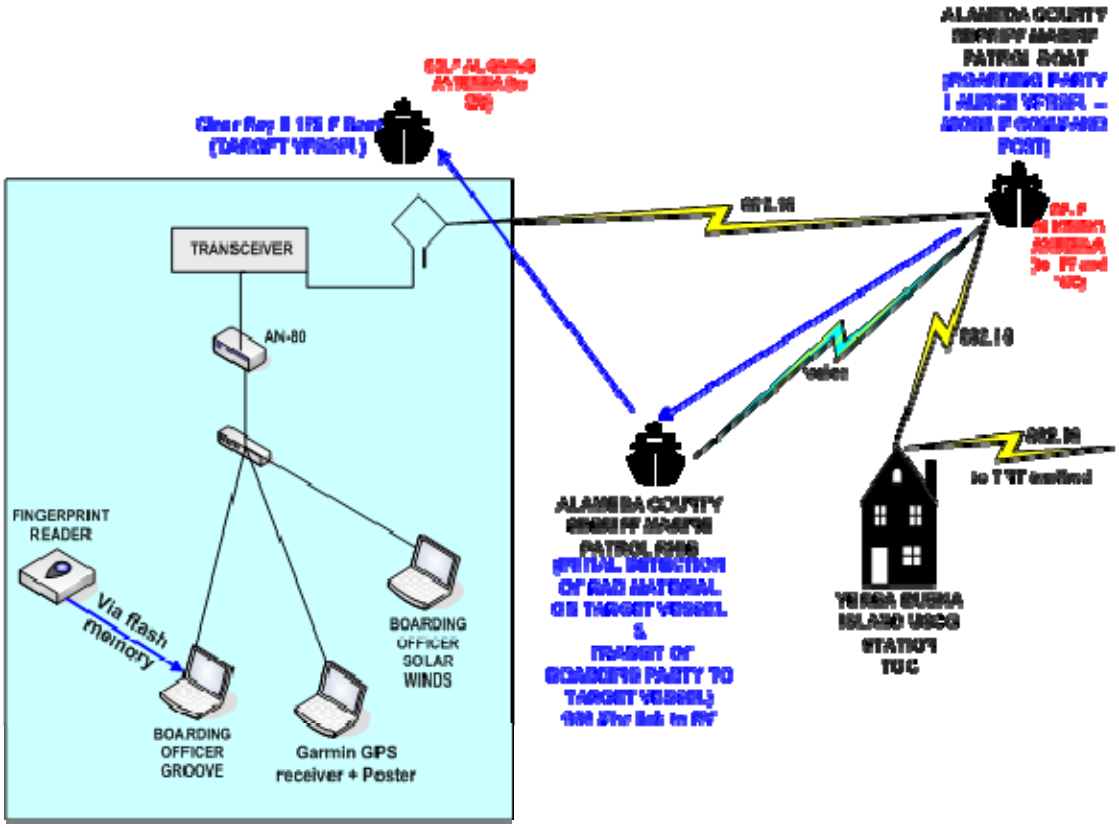

Figure 20. TNT MIO 07-1 Network in San Francisco Bay Area (From TNT 07-1 AAR)

I. TNT MIO 07-2

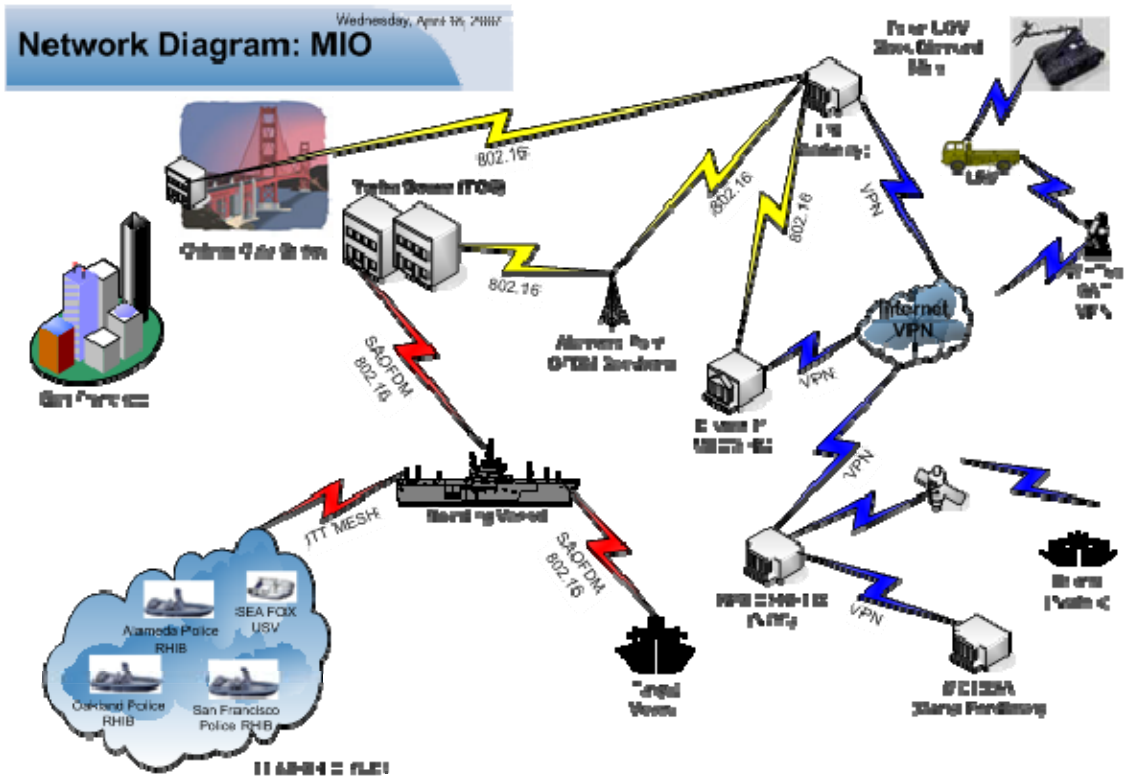

Figure 21. TNT MIO 07-2 Network in SF Bay Area
(From TNT 07-2 AAR)

This experiment introduced the ITT mesh-based drive-by radiation detection network, augmented by the Sky Pilot system, capable of providing higher transmission rates. Figure 22 below illustrates the Sky Pilot setup on the SFPD Marine Unit Boat. The Sky Pilot network expanded the MIO collaborative environment to the Marine unit in the port service area to allow them to participate. This experiment further proved the reliability of using the Sea Fox USV in a collaborative MIO environment.

Figure 22. Sky Pilot Networking Node Setup on the SFPD MU Boat (From TNT 07-2 AAR)

- Network Technology
    - MIMO OFDM 802.16 link was explored as ship-to-shore extension to GG Bridge node for open waters environment. The application goal was to enable video feed from the TV approaching

the GG Bridge and SF Bay. The video feed failed, but the link demonstrated strong performance at 100 Mbps level from as far as 10 nm to GG Bridge

  - Fixed OFDM 802.16 backbone stretched out to the GGB site for ship-to-shore link in open waters.
  - SAOFDM/802.16 for BV to TOC and BV to TV links
  - ITT Mesh for Sea Fox USV and Oakland Police Marine Unit network for drive-by radiation detection
  - Iridium Link for radiation sensor file transmission
  - Quadro Iridium Solution for Underground Vehicle (UGV) video
  - Integration of LRV, Sky Pilot, and Geo-Satellite Link for UGV high quality video

- Sensors
  - ARAM
  - Swedish CBRN Vest
- Collaboration Tools
  - Groove
  - NPS SA Multi-Agent System
  - NPS VC1
  - Swedish CBRN Vest
- Results
  - The new self-aligning broad band wireless solutions supported boarding and target vessels on-the-move with critical 2-3 nm distances between the vessels.

- MIO Fixed OFDM 802.16 backbone stretched out to Golden Gate Bridge site was stable with strong signal to LBNL relay.
- Biometrics identification with forward deployed data base latency less than 1 min
- Depiction of biometrics identification in SA view, geolocationally synchronized
- Rapid introduction of chat spaces (two hour adaptation cycle) for substituting failed Groove shared environment
- Remote video demonstration of Sensor Vest from Sweden (drive-by detection simulation)
- End-to-end networking with Radiation Detection sensors during drive-by and Boarding Party search phases resulted in six out of six sources correct finding and identification, which is the best MIO 2006-2007 result so far
- The forward deployed biometrics data base allowed CG Boarding Officers to fit the biometrics identification technique in their boarding procedures
- The TOC was able to receive the Sea Fox video of the target vessel from different positions, circling around the target vessel.

- Conclusion
  - The USV operators learned vital lessons of how to control the Sea Fox from the Alameda County Sheriff's fast RHIB.
  - The Sky Pilot broadband mesh network allowed extension of the MIO collaborative environment to the USMC unit conducting search of individuals planting a radiation source in the port service area and proved to be feasible for ship-to-shore communications.

- The LLNL team achieved higher levels of performance in drive-by radiation and explosive detection combined with geographically distributed analysis.
- The overseas sites achieved a more advanced level of multiple video feeds and collaboration and data sharing with MIO participants.

J. TNT MIO 07-3

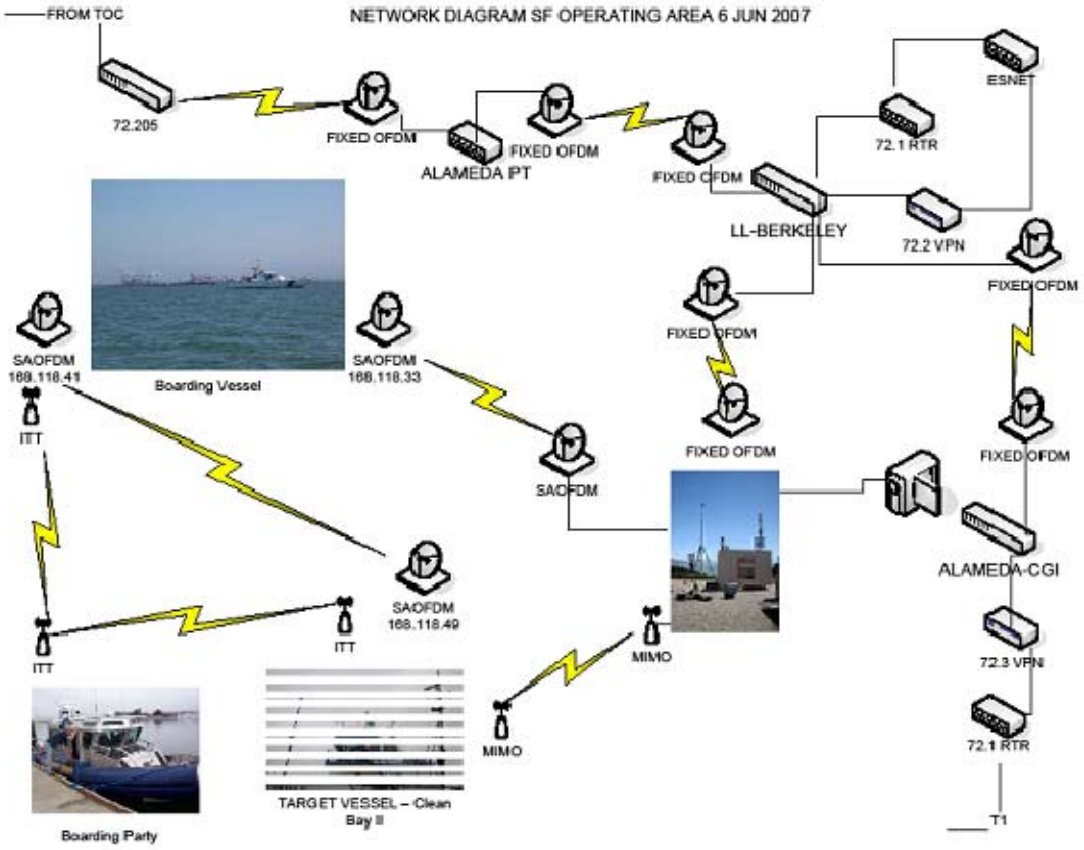

Figure 23. 5/6 June San Francisco Bay Network Diagram
(From TNT MIO 07-3 AAR)

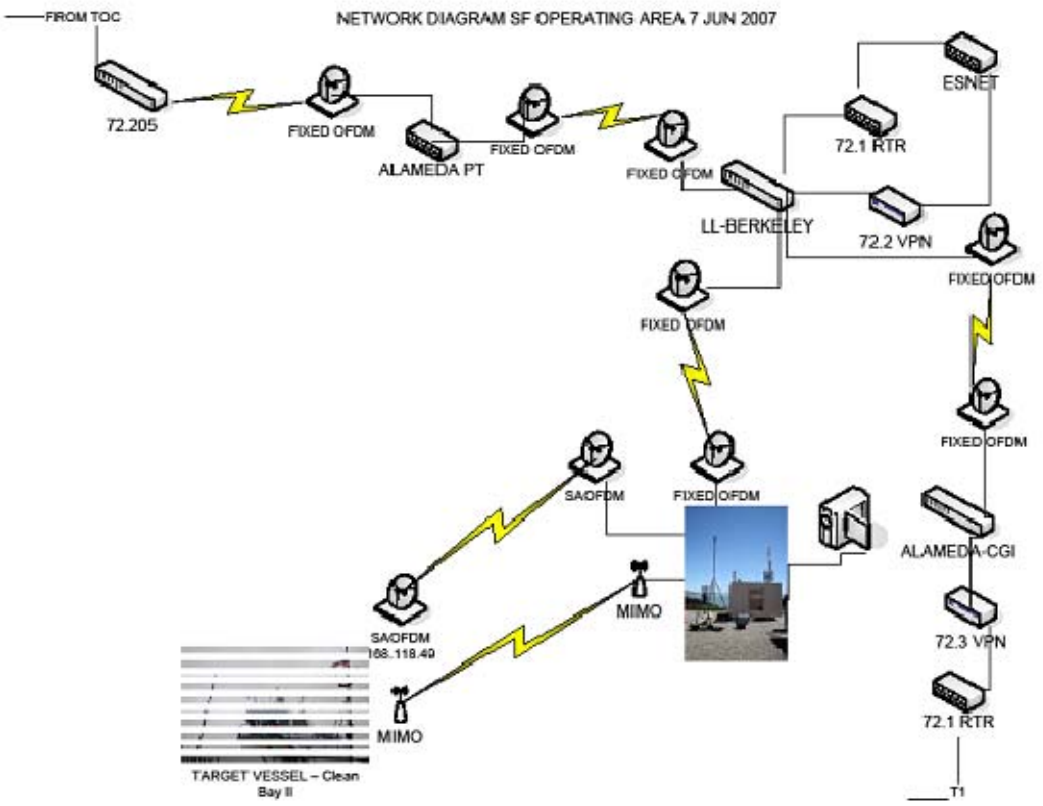

Figure 24. 7 June San Francisco Bay Network Diagram

(From TNT MIO 07-3 AAR)

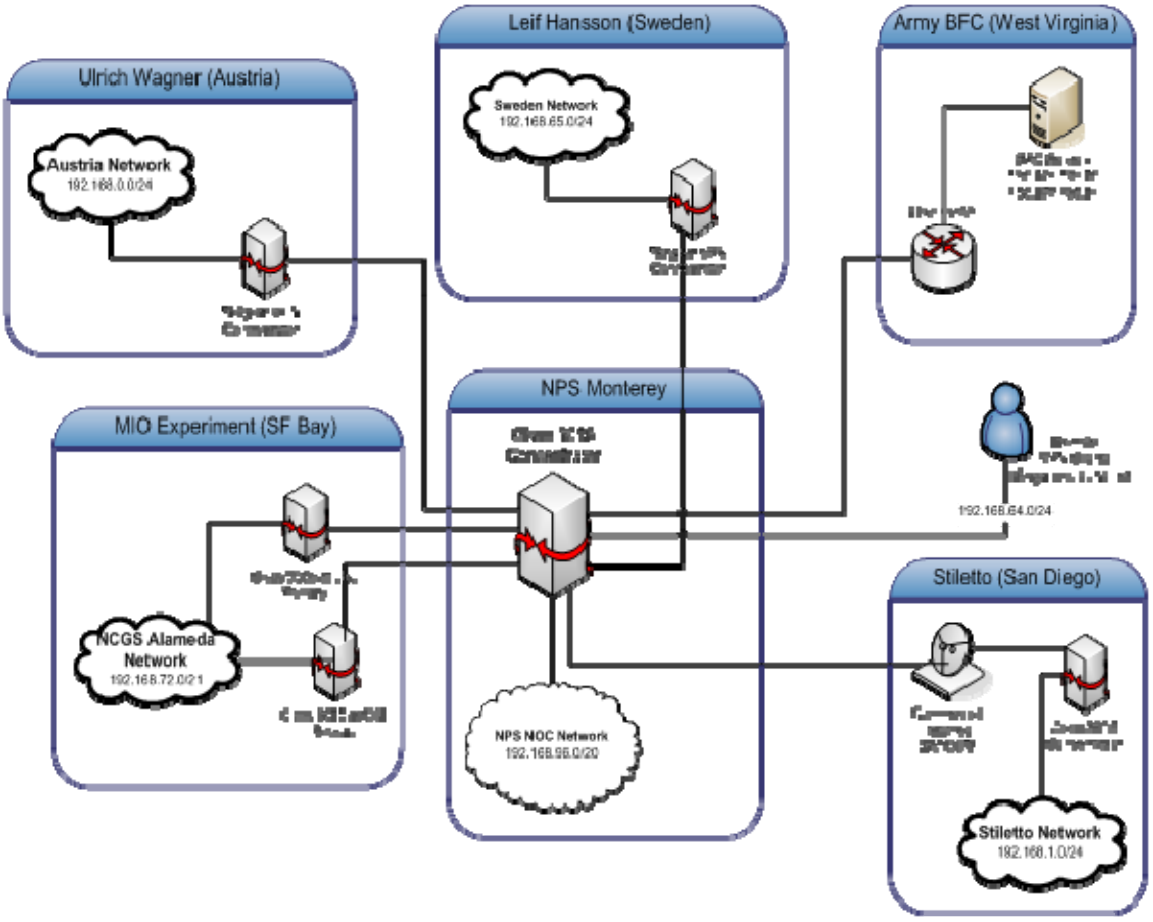

Figure 25. VPN Cloud Connecting MIO with Global Collaborators (From TNT 07-3 AAR)

This experiment was a repetition of the last. It was, however, a new perspective on the VPN's affect on the network. The VPN Concentrator at NPS was used as a hub in a hub-and-spoke architecture for purpose of simplicity and to remain a constant hub even though the nodes (or spokes) in this architecture may change over time. One of the issues was that the VPN concentrator at LBNL had its internet connection dropped due to the LBNL network's Intrusion Detection System falsely identifying the MIO's experiment traffic as an attack. The other issue was access list management for all VPN connections. The hub-and-spoke architecture makes the access list configuration for shared IP address time-consuming and prone to errors. This was more noticeable for the Sky Pilot and Sea Fox arbitrary networks, for which the VPN architecture was not configured to handle.

The recommendations made were to have a pre-established network map for all participating networks, in order to expedite access list configuration. The other recommendation was to adjust the VPN architecture to accept dynamic allocation of networks between different sites.

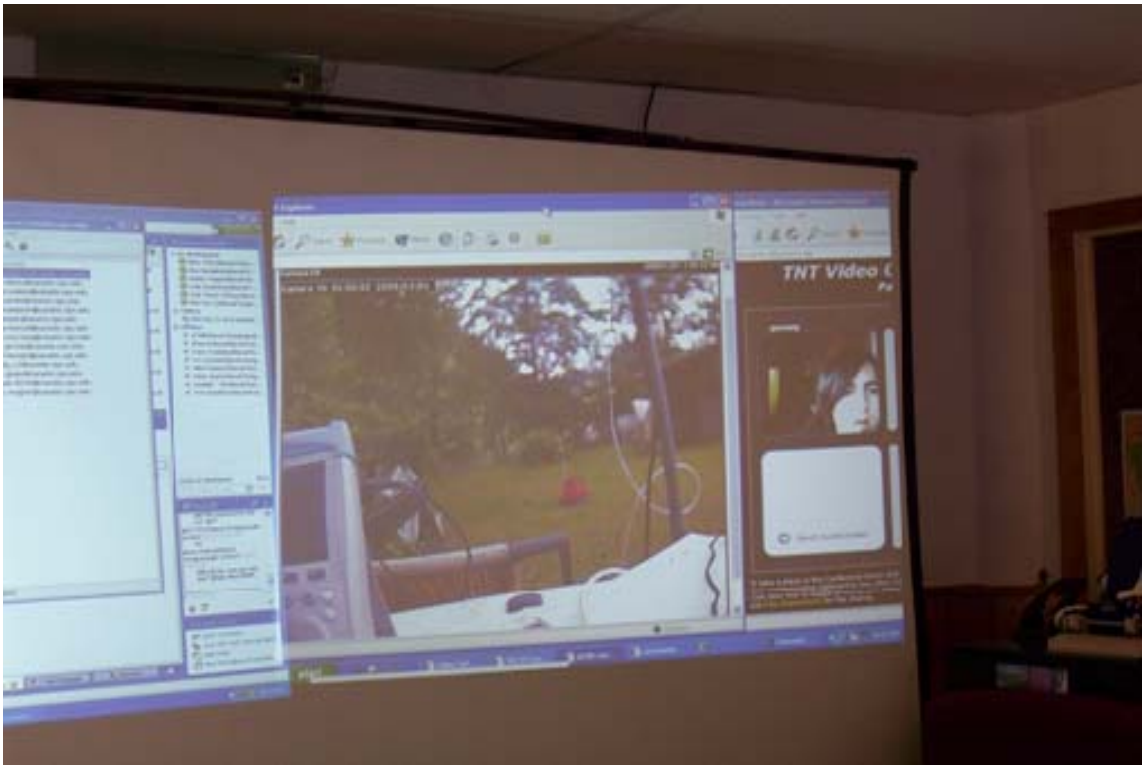

Figure 26. YBI NOC Showing Austria and Germany Video Feed
(From TNT 07-3 AAR)

Figure 27. YBI NOC Showing Video Feed from Boarding Vessel on 6 June (From TNT 07-3 AAR)

- Network Technology
    - SAOFDM/802.16 between BV and TV and between BV and GGB
    - Fixed OFDM/802.16 between GGB and LBNL, between LBNL and CGI Alameda, and between LBNL and Alameda PT
    - MIMO between GGB and TV
    - ITT Mesh between BV and BP RHIB and between TV and BP RHIB

- Sensors
    - ARAM
- Collaborative Tools
    - Groove
    - NPS SA Multi-Agent System
    - Jabber
    - NPS VC1
    - EWall
- Results
    - Radiation file posting to Groove Workspace caused confusion due to same file used for both days of experiment.
    - Cell phone was used by the BP to inform YBI NOC of updates, which YBI NOC then posted to Jabber's discussion area.
    - NPS VC1 was used by Austria and LLWO to post or view radiation files and live video.
    - Clear and stable video from the BV to the YBI NOC via successful SAOFDM link between BV and the GGB.
    - ITT Mesh established between BV and TV.
    - 802.16/OFDM links with mobile nodes, like the BV and TV, was problematic, but successful with all other fixed nodes.
    - Groove Workspace confusion was mitigated by using one workspace per day. A separate chat window was used to handle network administration trouble calls with Austria.
    - Headquarters (HQ) was able to quickly provide guidance to BP, once information was posted to Groove Workspace by Austria and LBNL.

- Clear, steady, and reliable video received from Austria and GGB. See figure 26.
- Quick response time for posting and acknowledgment of discussion threads.
- Radiation file retrieval and analysis between Austria and LBNL was processed within one and a half hours. Discussions were used to inform necessary nodes of file posting.
- Jabber was used for discussion and SA Agent used for file posting among participants on the second day of experiments due to lack of Groove synchronization.
- Using Google Earth and VPN connection with Austria/Germany border station, suspect movement was accurately tracked.
- Files and discussion from the BP was synchronized with the Groove Workspace maintained by YBI TOC
- All information received via cell phone from BP was posted to Groove Workspace for all other participants to observe.
- BP could not post files to Groove Workspace, therefore they could only communicate information via cell phone. This was a result of no LOS path between GGB SAOFDM and BV SAOFDM due to disrupted 900 MHz control signal for GGB SAOFDM near metropolitan area.
- LBNL able to retrieve Austria's radiation files
- Information flow and radiation files from Austria successfully posted

- Severe noise effects encountered by the MIMO segment highlight the fact that it should be a well aligned directional solution. This is exactly what SAOFDM does in the most accurate adaptive way.
- The border control simulation site in Bavarian Alps produced full scale video and radiation detection feed during the building search and check point control. For the first time the radiation detection script was generated by local source unknown to LLNL experts and was successfully decodes within several minutes.
- The HQ C2 Cell was formed as a part of the MIO test-bed environment. It produced detailed analysis for the MOTR plan based C2 activities integration and provided foundation for interagency coordination scenario elements.

- Conclusion
  - New solutions for bridging different collaborative technology platforms (Groove, Jabber, EWall, and NPS VC Tool) for going across hierarchical boundaries were revealed during the extensive data sharing process with the checkpoint site in Bavarian Alps.
  - The drive-by detection in the open waters revealed best benefits of the ITT mesh solution for RHIB-Boarding vessel communications. It worked perfectly during the first day, marked by the very rough waters, and delivered good data sharing quality.
  - Groove synchronization must be done prior to experiment. Otherwise, Jabber and NPS CENETIX Video Conference Room serve as excellent redundant data-sharing media to keep every node informed.

- MIMO needs to have well aligned directional antennas in order to provide better link connectivity.
- 900 MHz is a problematic frequency to control SAOFDM antennas in areas dominated by an abundance of 900 MHz range signals from cellular phones.

K. TNT MIO 07-4

During TNT MIO 07-4, the objective was the same as before. However, the particular focus of TNT MIO 07-4 was on networking and data sharing solutions. This was enabled by using multiple small craft interdiction teams to rapidly respond to nuclear radiation threats in the San Francisco bay area. (TNT 07-4 AAR) In addition to the bay area, two other areas were included, outside the GGB and the Vallejo Riverine area. This expansion of the MIO operational environment was necessary to further evaluate the implementation of network equipment and collaboration tools to reach the objectives.

The "challenge was to allow all parties, while the searches were in progress, to share live video feeds, emanating radiation data, and biometric information with experts to form possible connections with known threats." Furthermore, "providing continuing two-way video sharing between the Riverine site and the YBI TOC appeared to be problematic due to the network congestion." (TNT 07-4 AAR)

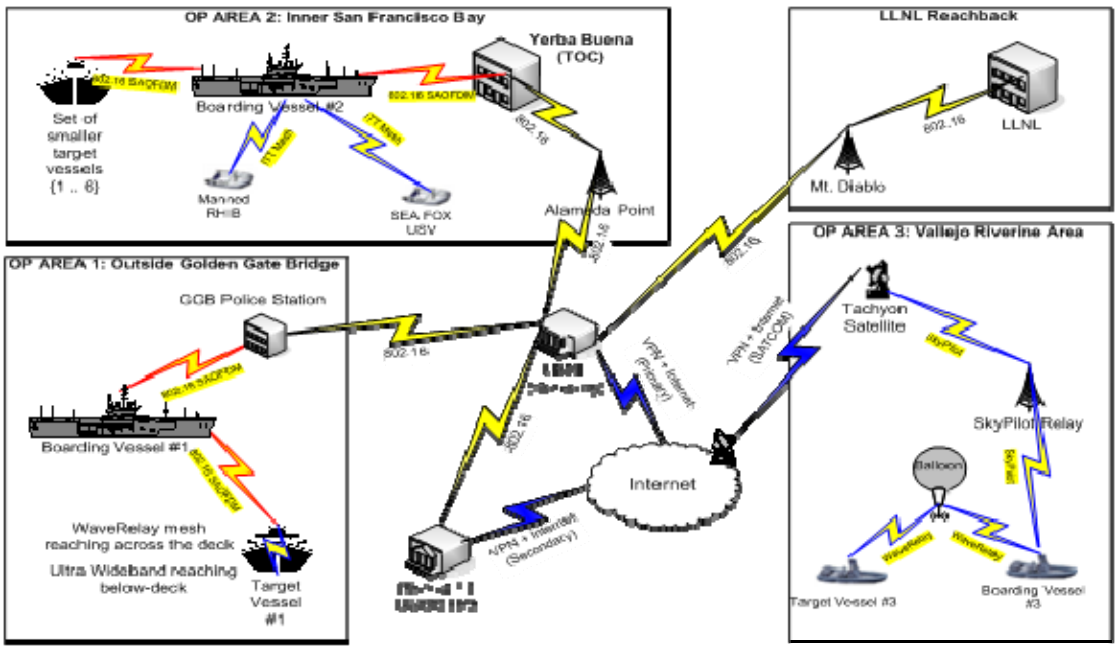

Figure 28. TNT MIO 07-4 Network Topology

(From TNT 07-4 AAR)

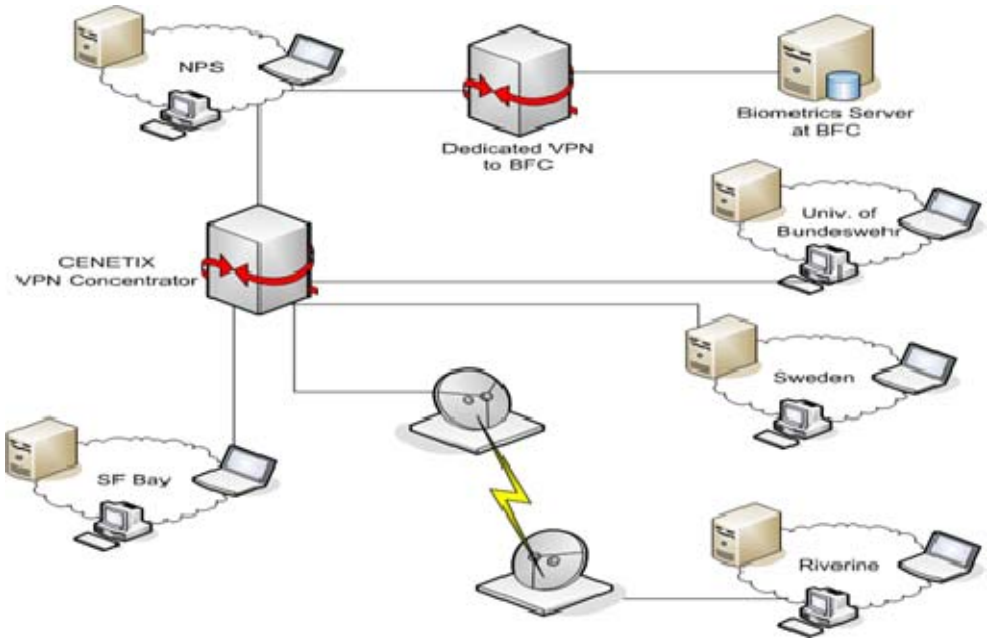

Figure 29. Diagram of VPN Topology Used in TNT MIO 07-4

(From TNT MIO 07-4 AAR)

- Network Technology
    - SAOFDM/802.16, OPAREA ONE: between BV and TV and between BV and GGB, OPAREA TWO: between BV and TV and between BV and YBI TOC
    - Fixed OFDM/802.16 between GGB and LBNL, between LBNL and District 11 USCG HQ, and between LBNL and Alameda Pt, between Alameda Pt and YBI TOC, between LBNL and Mt. Diablo, and between Mt. Diablo and LLNL
    - ITT Mesh, OPAREA TWO: between BP RHIB and BV, and between Sea Fox (USV) and BV
    - Sky Pilot, OPAREA THREE: between Tachyon Satellite and Sky Pilot Relay and between Sky Pilot Relay and BV
    - Wave Relay, OPAREA THREE: between BV and Balloon and between Balloon and TV
- Sensors
    - ARAM on Sea Fox and USCG Tern's RHIB
    - Chemical, Biological, Radiological, Nuclear (CBRN) Vest
- Collaborative Tools
    - Groove
    - Jabber
    - NPS SA Multi-Agent System
    - NPS VC1
    - Blue Force Tracker (BFT)
    - EWall

- Results
    - Based on the intelligence received earlier and the alerts posted by the monitoring center the first small craft was intercepted in the open waters west of Golden Gate Bridge, simulating the site in NY Harbor. Simultaneously the second small craft was intercepted in the S.F. Bay and searched for nuclear devices. Also simultaneously, the third target vessel was found and interdicted in the S.F. Bay riverine area.
    - ARAM systems aboard the Sea Fox and the USCGC Tern's RHB did drive-bys looking at the Bowling Ball plutonium surrogate, a smoke detector that uses Ra-226, and some Depleted Uranium (DU) counter weights. Four (4) of the six (6) red alarms for Pu also included proper identification (the other two Identified as Uranium and Americium).
    - This was the first experiment in which real-time emergency response coordination was executed between the HQ C2 (simulation for District 11) and PANYNJ responders based on MOTR recommendations. This was accomplished by means of networking between the SF Bay boarding parties (simulation for the event in NY Harbor) and collaboration between HQ C2 and PANYNJ via the NPS SA and PANYNJ JSA system.

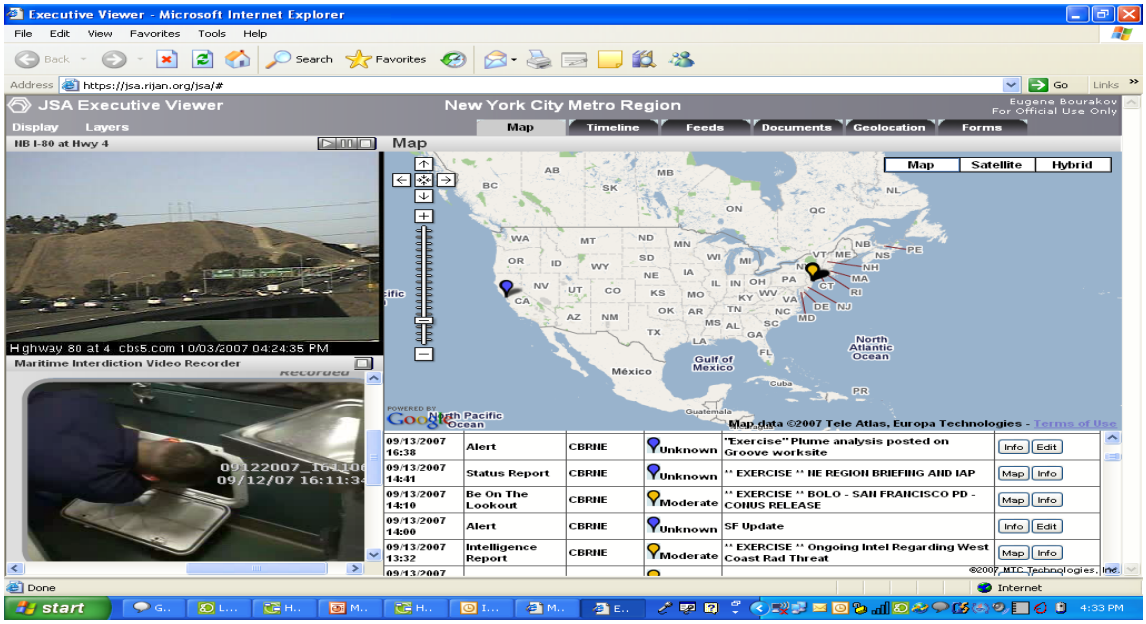

Figure 30. Video feed of SF Bay Interdiction Events into the PANYNJ JSA Tool (From TNT MIO 07-4 AAR)

- Multiplatform control link enabling directional broadband OFDM network forming on-the-move was used by alternating 900 MHz, SMS-GPRS (cellular), and Iridium satellite links.
- The VPN infrastructure was also extended across a commercial satellite link into the riverine operating area inside San Francisco Bay, further stretching into the tactical last-mile solution space.
- The CBRN's ad-hoc network was able to deploy in a new environment; remote participants were able to communicate with CBRN vest; and data collected from the CBRN vest. See Figure 33 below to see how CBRN fit into the MIO network.
- The air balloon was able to relay between the Riverine network and the police boat on-the-move.
- Biometrics data sharing and alert propagation achieved with Sweden and HLS response system in PANYNJ Center.
- Clear video from NPS TOC was available.

- Biometric files posted successfully.
- Swedish Naval Warfare Center (SNWC) TOC able to send video.
- SA of BFT was available through the Internet.
- Swedish CBRN vest with BFT had successful communications via Turbo 3G. Swedish were able to successfully post biometric files into workspace and showed BFT on an interactive webpage. Figure 35 shows the connection diagram for SNWC CBRN vest.

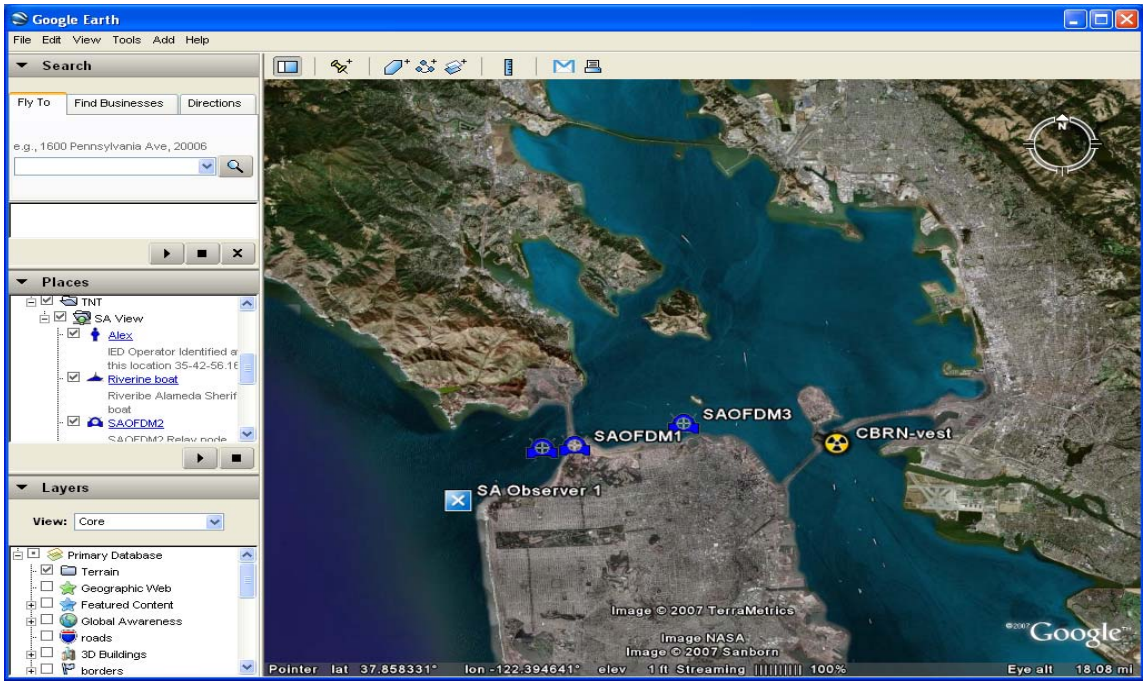

Figure 31. SAOFDM Nodes in SF Bay while Conducting Simultaneous Searches (From TNT MIO 07-4 AAR)

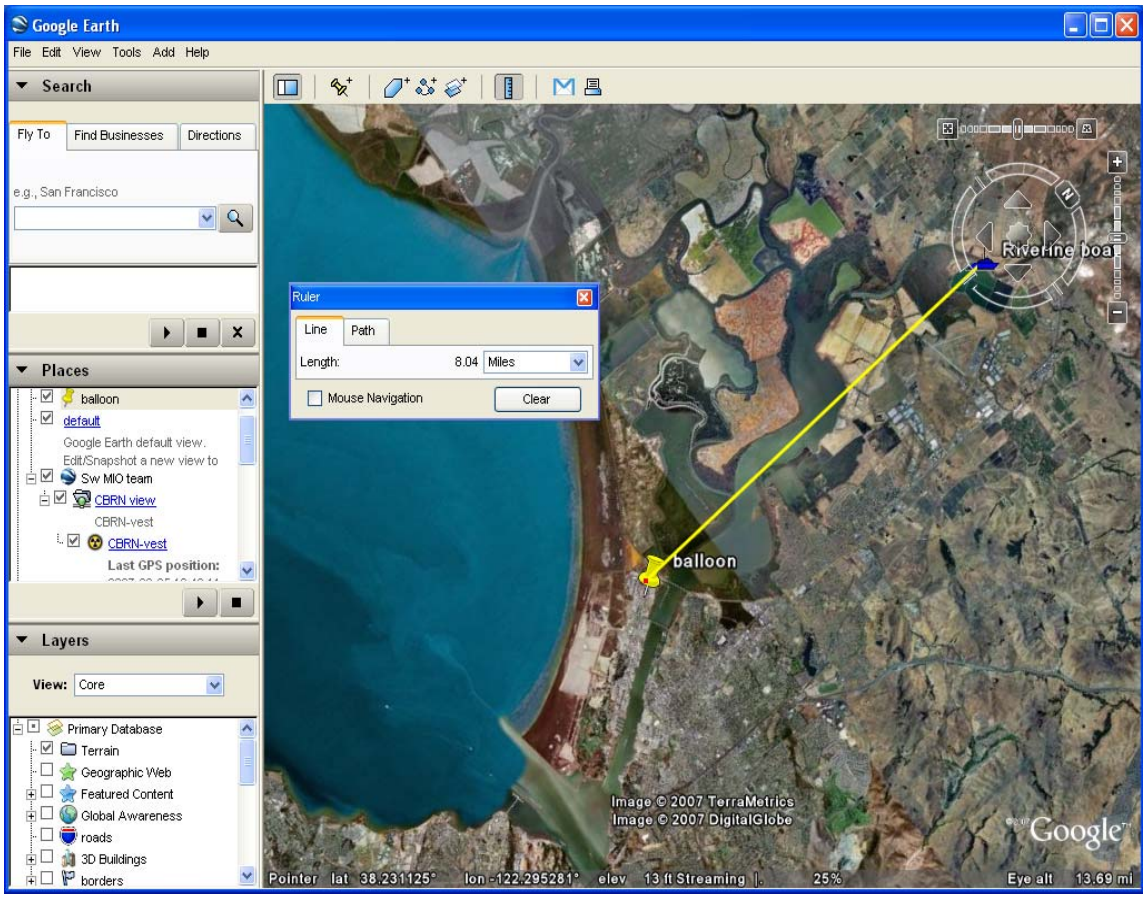

Figure 32. Linking the Riverine BV to MIO Network via SkyPilot (From TNT MIO 07-4 AAR)

- Conclusion
    - Integrating broadband MIO network on-the-move for small craft Radiation/nuclear network-controlled detection and ship-to-ship broadband networking in the open waters worked well.
    - Proving feasibility of simultaneous interdiction and data sharing between boarding events conducted in the open waters, inside the bay, and riverine area.
    - Integrating unmanned assets (Sea Fox), which actively participated in conducting drive-by detection with nuclear/radiation sensor onboard (Sea Fox) and relaying the riverine network to the police boat on-the-move via the aerostat
    - Achieving biometrics data sharing and alert propagation with the overseas site in Sweden and HLS response system in PANYNJ Center
    - The HQ C2, riverine network segments in the VUSD area, and the HLS PANYNJ site became new "nodes" of the MIO test bed. Additionally, the projectile-based sensor survived the landing and was able to communicate afterwards.
    - Some of the solutions for simultaneous video feeds sharing between boarding parties didn't work as expected, providing us with good lessons learned for the subsequent application networking improvement.
    - All links worked successfully with no observed downtime or significant configuration issues.
    - Simultaneous video feed from boarding teams did not work out.

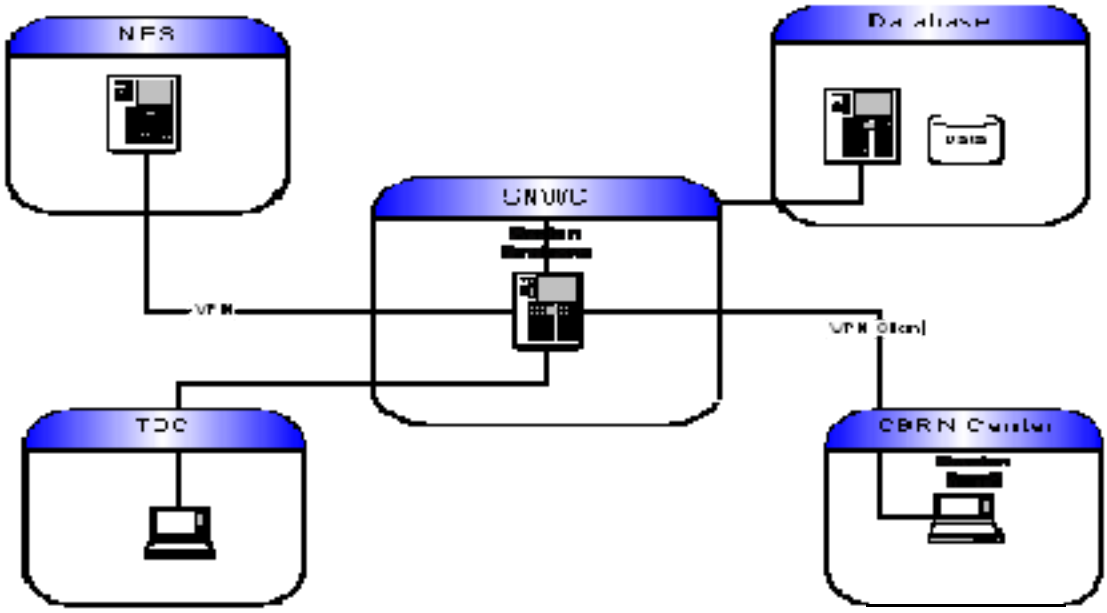

Figure 33. Network in Sweden and its Connection to MIO

(From TNT 07-4 AAR)

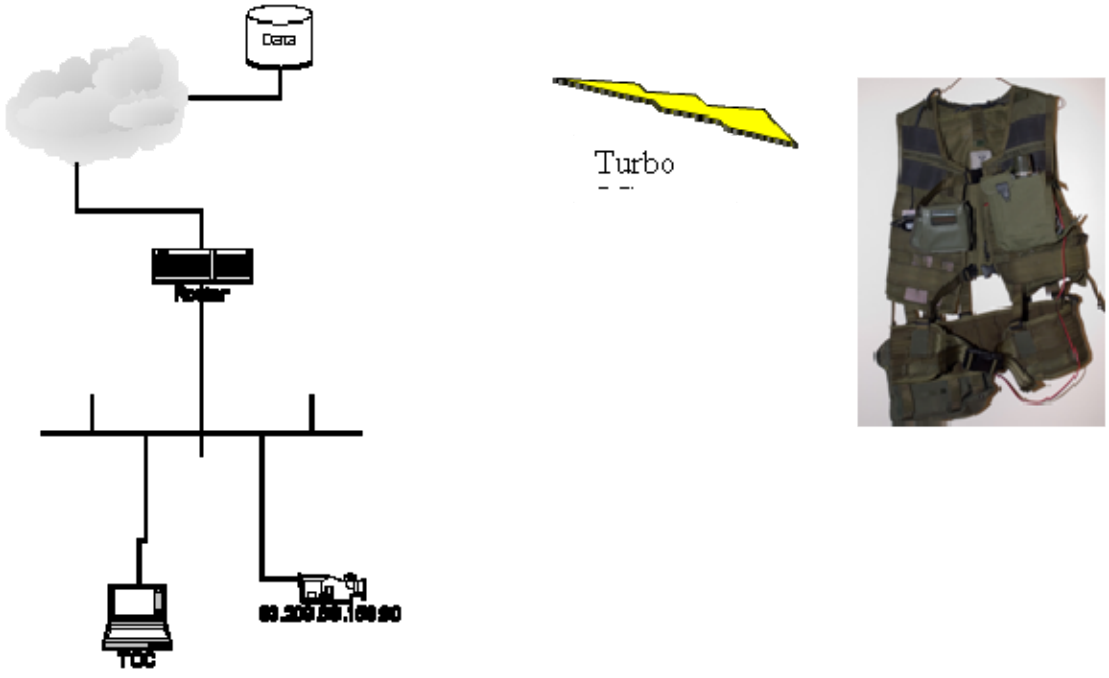

Figure 34. CBRN Vest and SNWC TOC

(From TNT 07-4 AAR)

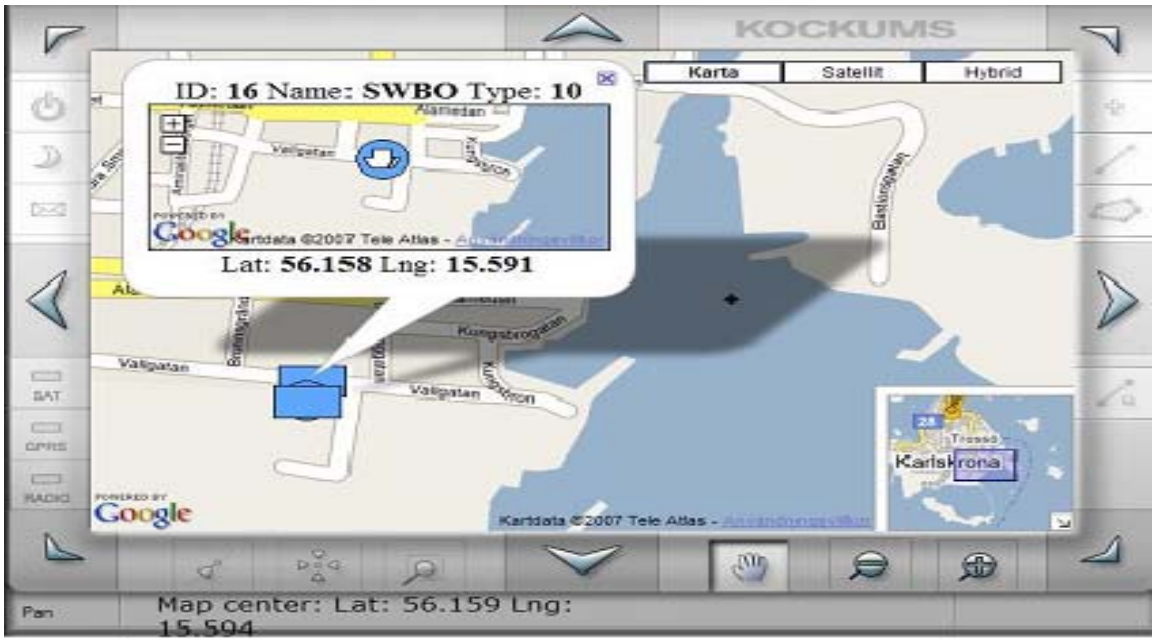

Figure 35. Example of The BFT Application

(From TNT 07-4 AAR)

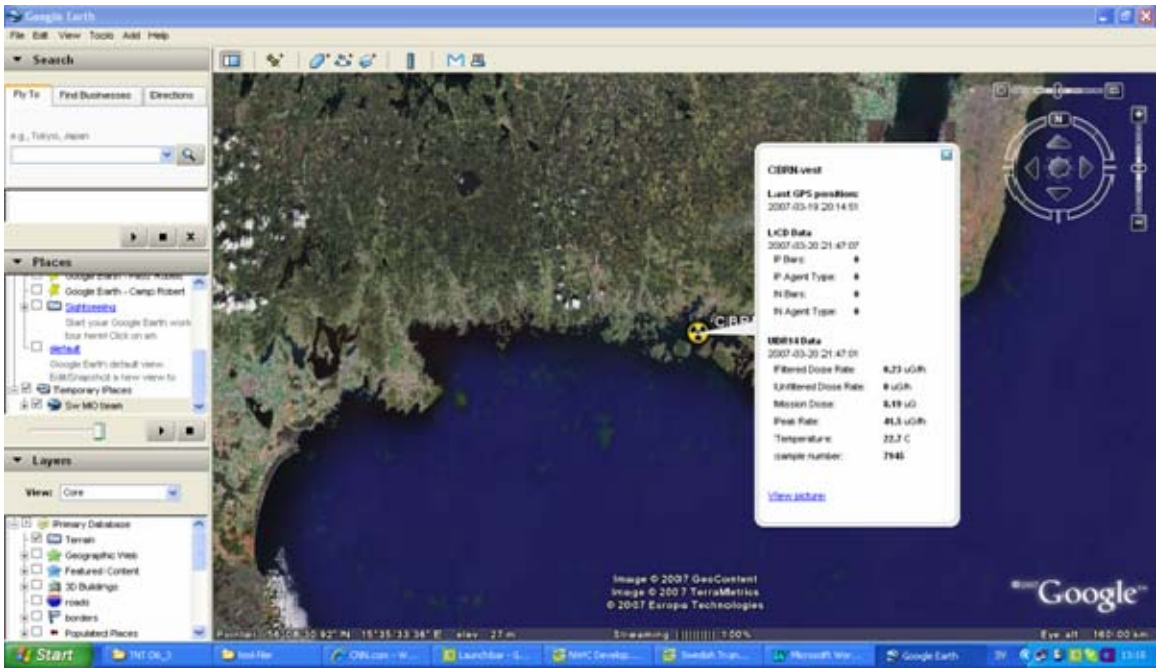

Figure 36. Tactical Operations Center View of CBRN Vest Data

(From TNT 07-4 AAR)

L. TNT MIO 08-1

- Network Technology
    - SAOFDM/802.16, OPAREA ONE: between BV and TV and between BV and GGB, OPAREA TWO: between BV and TV and between BV and YBI TOC
    - Fixed OFDM/802.16 between GGB and LBNL, between LBNL and District 11 USCG HQ, and between LBNL and Alameda Pt, between Alameda Pt and YBI TOC, between LBNL and Mt. Diablo, and between Mt. Diablo and LLNL
    - ITT Mesh, OPAREA TWO: between BP RHIB and BV, and between Sea Fox (USV) and BV
    - Sky Pilot, OPAREA THREE: between Tachyon Satellite and Sky Pilot Relay and between Sky Pilot Relay and BV
    - Wave Relay, OPAREA THREE: between BV and Balloon and between Balloon and TV
- Sensors
    - ARAM on Sea Fox and USCG Tern's RHIB
    - Chemical, Biological, Radiological, Nuclear (CBRN) Vest
- Collaborative Tools
    - Groove
    - Jabber
    - NPS VC1
    - NPS SA Multi-Agent System
    - Blue Force Tracker (BFT)
    - EWall

- Results
    - Directional antenna with wider angle beam (20 degree) is preferable since it easily establishes and maintains OFDM LOS link up to 5 Km and keeps it more reliable for mobile node scenarios.
- Conclusion
    - Redline radio and IMU connectors should be protected from possible water and dust damage.
    - SAOFDM antennas continue to be a better choice to maintain LOS.

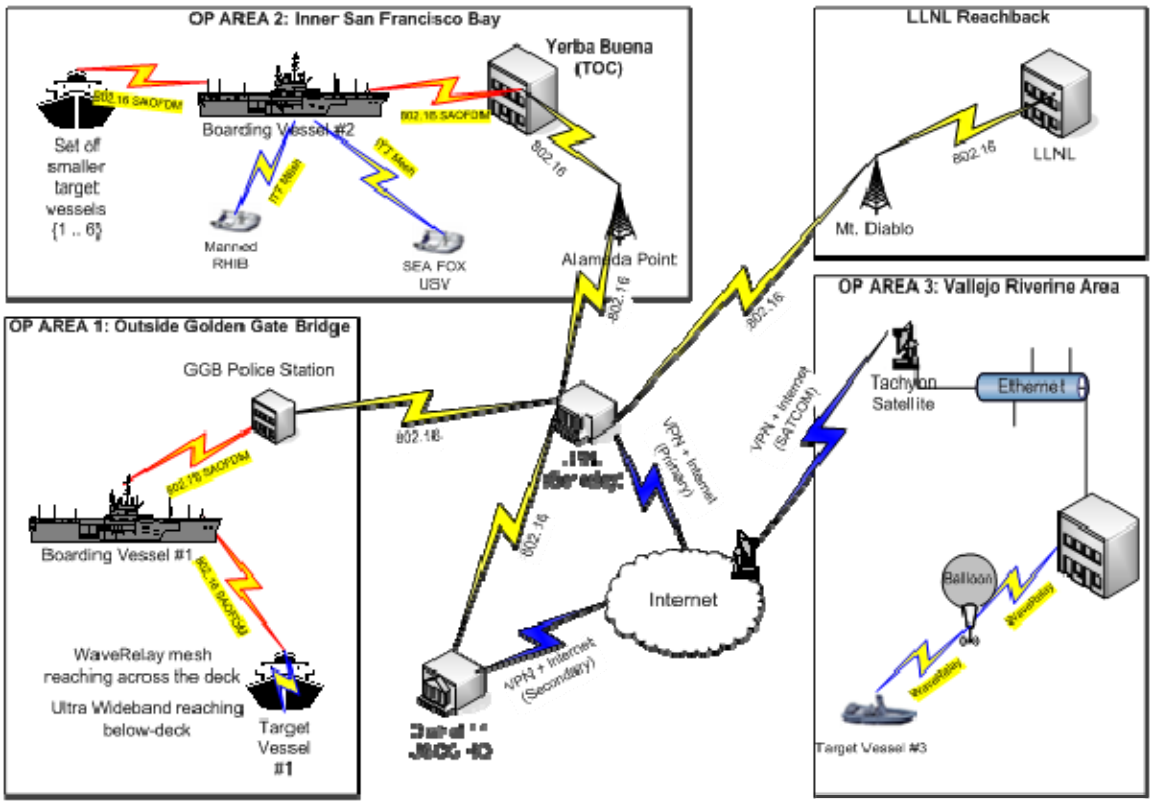

Figure 37. San Francisco Bay Topology

(From TNT 08-2 Planning Document)

M. SUMMARY ANALYSIS

- Recurring problems
    - Intermittent or loss of signal due to LOS problems from lack of self-aligning antennas, distance, natural obstacles, structures, or disrupted control signal (900 MHz).
    - Signal interference due to RFI or EMI
    - Improper data management, i.e. incorrect file naming or placement
    - Lack of proper hardware or software set up, i.e. NAT, VPN, and Groove not properly configured or installed on all remote node computers.
- Recurring Solutions
    - Self-aligning antennas
    - Wireless technology explored or added for redundancy or better performance, i.e. 802.16 over 802.11, 802.20, ITT Mesh, UWB, 900 MHz
    - Collaboration tools added for redundancy or explored for advantages, i.e. Groove, SA Multi-Agent System, VC1, CBRN, EWall, BFT, Jabber, Cell Phones
    - Adding more nodes to contribute or to analyze intelligence.

By looking at the results and conclusions of the past MIO experiments, the trend of exploring new wireless technology to circumvent obstacles and the search for better collaborative tools to improve the data sharing process becomes apparent. From the MIO 05-2 experiment, the problems with establishing a link for data sharing became a priority. Whether it was a weak wireless link, like 802.11, being replaced with a more robust wireless link, like 802.16, or the manual alignment of OFDM antennas being replaced with self aligning ones for the mobile maritime nodes, the MIO experiments proved to explore better ways to establish links with maritime nodes from shore without hampering

the maritime node's mobility or distance necessary to search for nuclear or explosive materials. Furthermore, sharing near real time captured data from radiation sensors or biometric devices through the use of collaborative tools has also improved. Collaborative tools which handle video conferencing, file posting, or discussions can play a major part in keeping every node informed of the situation developing. Finally, the amount of data that must be analyzed must be carefully managed in order to avoid confusion or loss of valuable information. With every addition of a collaborative participant or target vessel, the human and technological assets must meet the demands to keep the operation moving efficiently. Thus, every MIO has explored that as more participants enter the MIO collaborative network to support, enhance, and expedite the DM process, the faster, more interoperable, easily accessible, and more reliable the link and collaborative tools have to be in order to meet the near real time data sharing requirements of the C2 element, MIO forces, and remote experts. Looking at Tables 1 and 2 below, one can see that the trend illustrates an increase in network technology, as more nodes from geographically distributed participate in more complex MIO scenarios. Furthermore, one can also see from Table 1 that the most interoperable collaborative tools and sensors must be explored in order to capture the data and share it with the other nodes in the network. It takes a single crack in the foundation of those assets to give the opportunity to terrorists or criminals to seep through and achieve their objectives.

The observations of past MIO experiments have shown that adding a riverine node should not be a challenge so much as a new area to explore the implementation of the technology and collaborative tools used. As the MIO experiments continue to expand to geographically distributed nodes, the riverine area should not be left out of the network, since it should contribute a last line of defense in the maritime environment. The assets for the riverine area should not be any less viable than in other areas. Furthermore, the riverine area should only be an application of what is known to work, to evaluate it for contribution to the network, and to find what adjustments need to be made to make this node more valuable in the data sharing process.

TABLE 1. MIO EXPERIMENTAL TREND		CONCEPT	MIO 05-2	MIO 05-3	MIO 05-4	MIO 06-1	MIO 06-2	MIO 06-3	MIO 06-4	MIO 07-1	MIO 07-2	MIO 07-3	MIO 07-4	MIO 08-1	MIO 08-2
	NETWORK TECHNOLOGY UTILIZED	802.11b	X												
		802.16/OFDM	X	X	X	X	X	X	X	X	X	X	X	X	X
		VPN	X	X	X	X	X	X	X	X	X	X	X	X	X
		UWB		X	X	X	X								
		Flash/OFDM 802.20					X	X	X						
		ITT MESH					X	X	X	X	X	X	X		
		900 MHz						X	X	X	X	X	X	X	X
		SAOFDM/802.16							X	X	X	X	X	X	X
		Sky Pilot System								X	X	X	X	X	X
		Sea Fox								X	X	X	X	X	X
		Satellite								X	X			X	X
		MIMO OFDM 802.16									X	X			
		Iridium Satellite									X	X	X	X	X
		Quadro Iridium									X	X			
		GPRS										X	X	X	X
		Air Balloon											X	X	X
		Wave Relay												X	X
	AREAS OF EXPERIMENTATION	Bay Areas	X	X	X	X	X	X	X	X	X	X	X	X	X
		Open Waters 3-5Nm WCGB										X	X		
		Riverine										X	X	X	X
	COLLABORATIVE TOOLS	Groove	X	X	X	X	X	X	X	X	X	X	X	X	X
		SA	X	X	X	X	X	X	X	X	X	X	X	X	X
		NPS VCI		X	X	X	X	X	X	X	X	X	X	X	X
		NPS Observer's Notepad							X	X	X	X	X	X	X
		MIT EWall						X	X	X	X				
		BFT									X	X			
		JABBER										X			
	RADIATION SENSORS & BIOMETRICS	Rad Pager	X				X								
		IdentiFINDER	X					X	X				X	X	X
		Neutron Pod	X												
		Oriec Device	X												
		GN-5		X	X	X									
		Biometric Fingerprint Reader			X	X	X	X	X	X	X	X	X	X	X
		Sodium Iodide								X					
		ARAM								X			X	X	X
		CBRN Vest									X	X			

Table 1. MIO Experimental Trend

		CONCEPT	MIO 05-2	MIO 05-3	MIO 05-4	MIO 06-1	MIO 06-2	MIO 06-3	MIO 06-4	MIO 07-1	MIO 07-2	MIO 07-3	MIO 07-4	MIO 08-1	MIO 08-2
DISTRIBUTED NODES	COLLABORATING SITES	AUSTRIA						X	X	X	X	X	X	X	X
		GERMANY										X	X	X	X
		DENMARK													X
		SWEDEN						X	X	X	X	X	X	X	X
		SINGAPORE							X		X	X	X	X	X
		TURKEY AF Academy													X
		USCG/D11						X	X	X	X	X	X	X	X
		USABFC/NBFC			X	X	X	X	X	X	X	X	X	X	X
		DTRA				X		X	X				X	X	X
		DOE-RAP						X	X	X		X	X	X	X
		LBNL					X	X		X	X	X	X	X	X
		LLNL	X	X	X	X	X	X	X	X	X	X	X	X	X
		IST	X	X	X	X									
		MCTSSA Camp Pendleton													
		OSD/HLD									X				
		TACSAT Washington, DC	X	X									X	X	X
		DNDO Observer													
		USSOCOM Observer					X	X	X	X	X	X	X	X	X
		NPS	X	X	X	X	X	X	X	X	X	X	X	X	X
		G.G. NATL REC. AREA U.S.								X	X	X	X	X	X
		PANY-NJ										X	X	X	X
		TOTAL	4	4	4	5	5	10	10	10	11	13	16	16	18
	SURFACE VESSELS	Alameda County Sheriff						X		X	X	X	X		X
		USCG	2	2	X	X	X	X	X	X	X	X	X	X	X
		San Francisco PD						X			X	X	X		X
		Sacramento/Vallejo										X			X
		OAKLAND POLICE							X		X	X	X		X
		LRV			X						X				
		OTHERS (O'Brien/Stiletto)	X	X			X		X	2	2	2			12
	UNMANNED NODES	Surface Vessels (USV/UGV)								X	2		X		X
		AERIAL (AEROSTAT)	X	X	X							X	X		X

Table 2. Distributed Nodes Trend

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RIVERINE PORTION OF TNT MIO 08-2 EXPERIMENT

Figure 38. World-Wide Network Topology
(From TNT 08-2 Planning Document)

A. OBJECTIVE

The main objective of the riverine portion of this experiment was to continue to utilize successfully tested rapidly-deployable wireless network equipment, radiation sensors, and collaborative tools, such as 900 MHz, ARAM, and NPS VC equipment, while collaborating with remote LLNL experts. Furthermore, the rapidly-deployable wireless network must be able to share that radiation data and video in near real time from the BV/CB with remote experts and decision makers, like LLNL and TOC personnel, in order to receive further guidance on the operation. This experiment would evaluate if the data sharing process in a more complex maritime environment would be successful with the abundance of data shared among the three operational areas and

remote experts and C2 node. Figures 39 and 40 illustrate the complexity of the network and geographic distribution of the nodes participating in the MIO scenario.

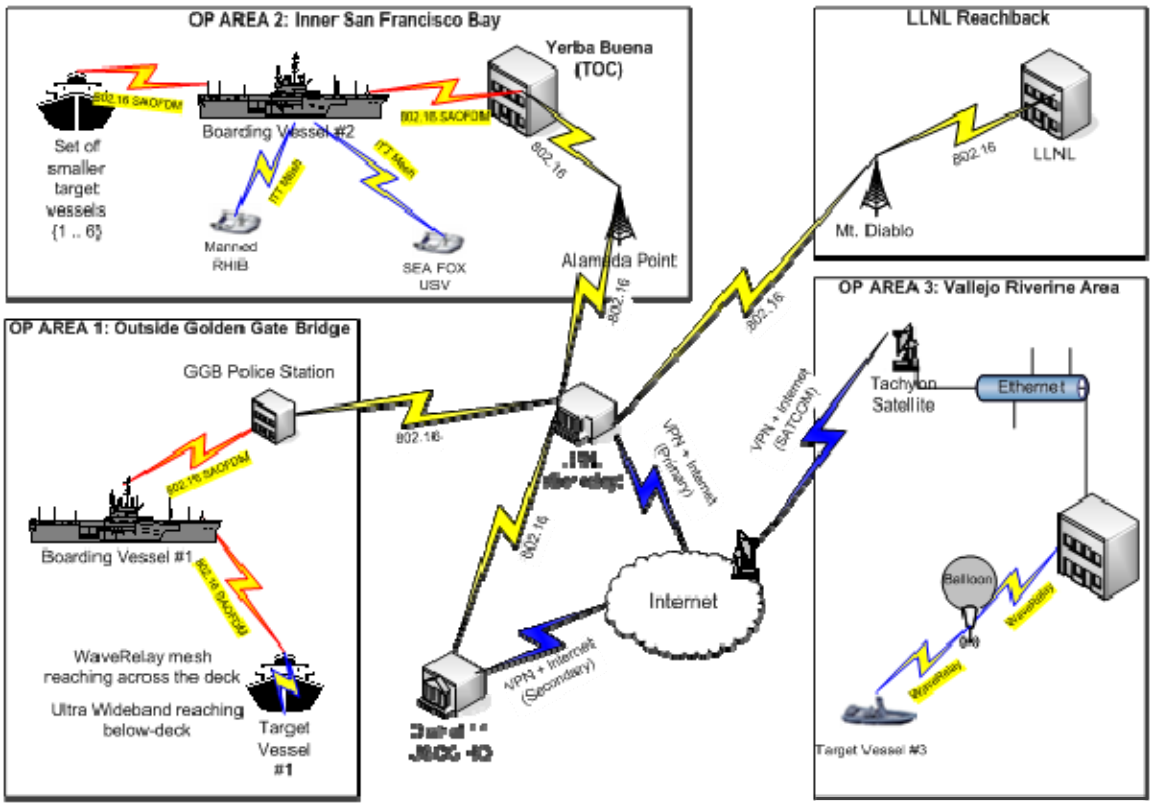

Figure 39. San Francisco Bay Topology for TNT MIO 08-2
(From TNT 08-2 Planning Document)

The following information describes the network infrastructure and collaboration tools used to keep every node in the loop. Figures 40 through 43 illustrate the environment and the set up to share data among the riverine unit and remote nodes.

- Network Technology
  - SAOFDM/802.16, OPAREA ONE: between BV and TV and between BV and GGB, OPAREA TWO: between BV and TV and between BV and YBI TOC
  - Fixed OFDM/802.16 between GGB and LBNL, between LBNL and District 11 USCG HQ, and between LBNL and Alameda Pt,

between Alameda Pt and YBI TOC, between LBNL and Mt. Diablo, and between Mt. Diablo and LLNL

- ITT Mesh, OPAREA TWO: between BP RHIB and BV, and between Sea Fox (USV) and BV
- Sky Pilot, OPAREA THREE: between Tachyon Satellite and Sky Pilot Relay and between Sky Pilot Relay and BV
- Wave Relay, OPAREA THREE: between BV and Balloon and between Balloon and TV

- Sensors
  - ARAM on Sea Fox and CB
- Collaborative Tools
  - Groove
  - SA Multi-Agent System
  - NPS VC

Figure 40. Google Earth View of SF Bay and Riverine Operation Areas (From Bourakov 2008)

Figure 41. YBI TOC Setup

(From Mercado, 2008)

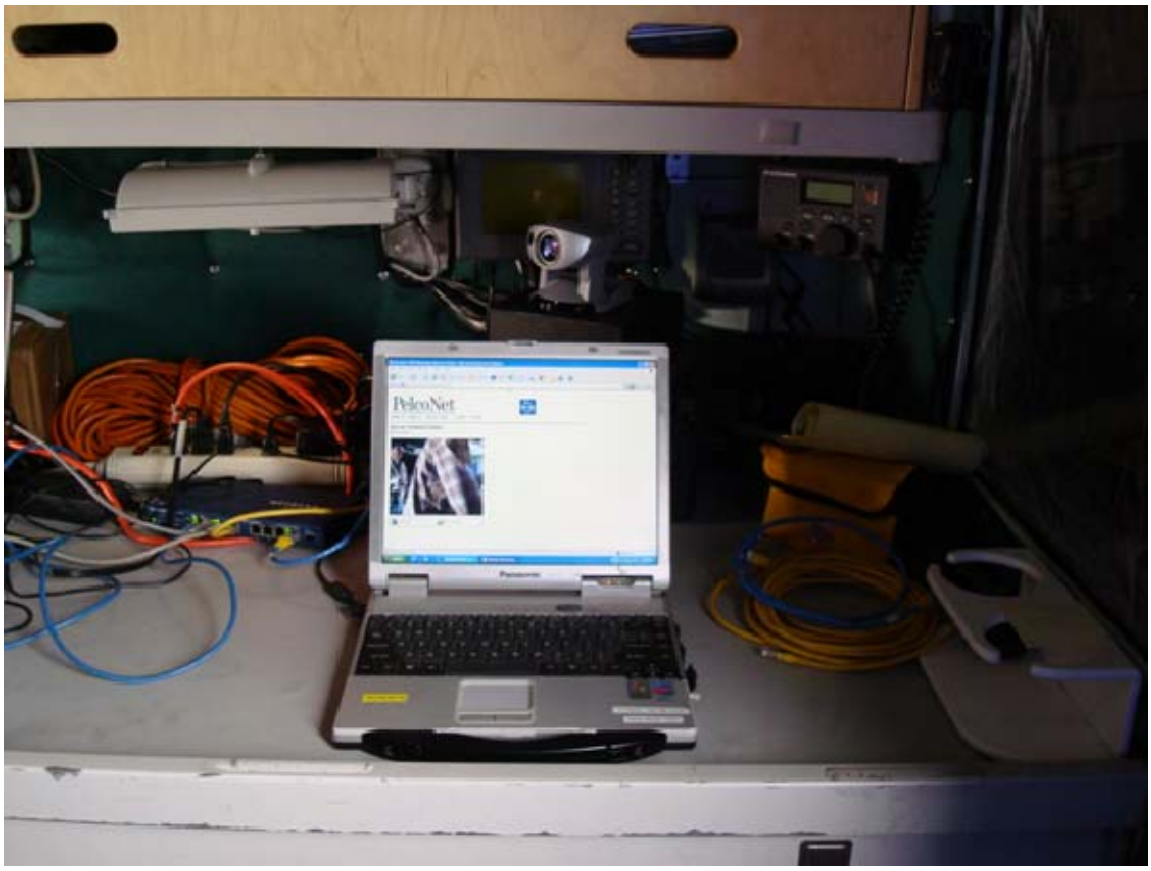

Figure 42. Alameda County Network and Video Conference Setup (From Mercado, 2008)

During the MIO Experiment, the equipment in the following figure was used to provide the 900 MHz link and the video conference capability to the BP in order to improve the SA and collaboration with remote experts. With the exception of the 900 MHz radio, which was built at NPS, the rest of the equipment can be purchased off the shelf. The problem, however, with commercial off the shelf (COTS) equipment is that it may not stand up to the rugged environment to which it is exposed either in a Riverine area or a dessert. Furthermore, the equipment's viability may be challenged by the weather elements, such as sea spray, snow, sand, or rain.

Eventually, the purpose of this experiment is to provide enough supporting data to convince the military and civilian law enforcement agencies to accept this technology for

field service and put into production a more rugged version, which will survive both the weather elements and rugged environments. Once this equipment is readily available to the law enforcement agencies, we can begin to see the expeditious enforcement of Riverine MIO operations. Furthermore, this technology and its implementation may find service in other areas of MIOs or land-based operations.

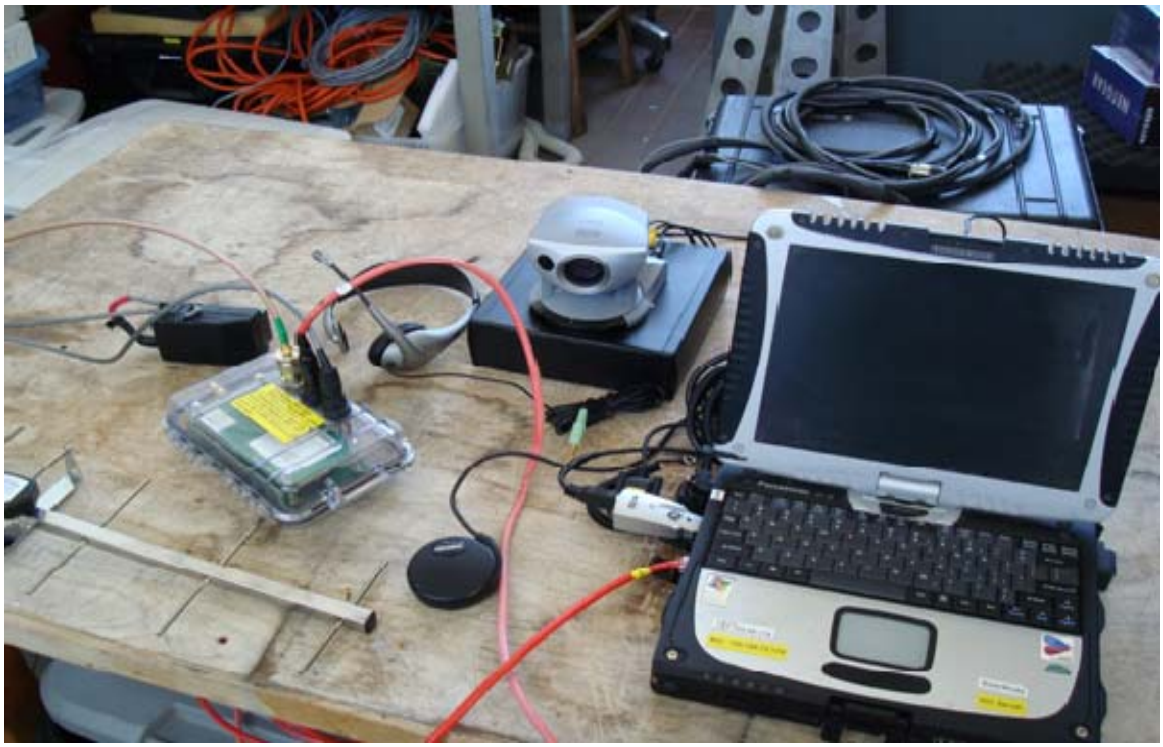

Figure 43. Riverine Network and Video Conference Equipment Setup (From Mercado, 2008)

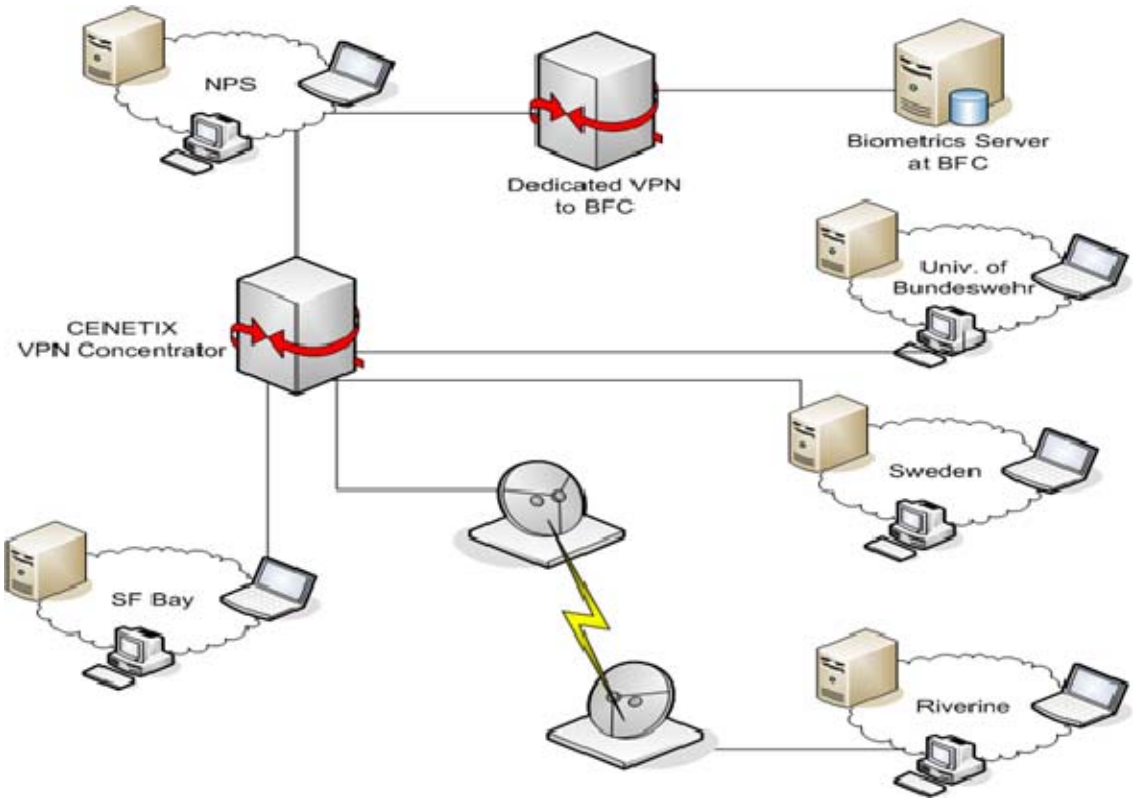

Figure 44. MIO Domestic and International Reach-back Network Topology (From TNT 07-4 AAR)

B. PARTICULAR FOCUS

The particular focus of the Vallejo Riverine node was to provide a link for the radiation data collected by the radiation sensor via the LLNL laptop back to the TOC and LLNL in near real time in addition to near real time video streaming. This link would provide the necessary data to enhance the SA for both the TOC and remote radiation experts at LLNL to give almost immediate feedback to the CB personnel of potentially dangerous radiation elements discovered in the Riverine target vessel. In addition, sharing the radiation data to remote experts through this link would help to keep the BP members focused on other aspects of the operations, like searching for any other illegal contraband, which may not emit any radiation, or collecting and reviewing the documents pertaining to the targets vessel and its crew. Figures 45 and 46 illustrate the radiation sensor and network set-ups.

Figure 45. Riverine CB with View of BP Network Set-up inside Canopy Area (After Netzer, 2008)

Due to the choppy waters and high winds experienced during the riverine portion of the experiment, the network set up had to be done inside the canopy to avoid exposing the laptop and peripheral equipment to water. The Yagi antenna was manually held by BP personnel outside the canopy to keep it pointed in the LOS of the balloon relay during the transit up and down the river.

Figure 46. Riverine CB with View of Radiation Sensor on Port Side of Canopy (After Netzer, 2008)

C. MAJOR RESULTS AND CHALLENGES

The major results of this portion of the MIO experiment was that it was able to confirm a 900 MHz link between the Riverine unit back to the ground station through a 900 MHz balloon relay, which allowed the TOC to capture and share the CB position information via the GPS position poster and NPS SA Agent and video streaming in addition to allowing the CB to capture video from a remote Pelco camera on the San Francisco bay TV through the 802.16/SAOFDM link. Furthermore, during the transit, the CB was able to view and participate with remote nodes using chat available through NPS VC. Figure 47 below illustrates a snapshot of the video streaming from the CB along the river. The maximum range of 900 MHz connectivity from the CB to the balloon relay was approximately 3.5 miles. Figure 48 below illustrates the CB's path from the pier at USCG Station in Rio Vista down the river before returning, after capturing radiation data from the TV during a drive-by. The breaks in the path are loss of

GPS posting connectivity due to loss of 900 MHz link or disconnection of the GPS sensor from laptop during transit through choppy waters. Figure 49 illustrates the snapshot of the video streaming from the S.F. bay TV, which was available through the internet by typing the camera's IP address into the URL space of the internet browser.

Figure 47. Snapshot of SA Agent View of Riverine CB Video Feed (From Bourakov, 2008)

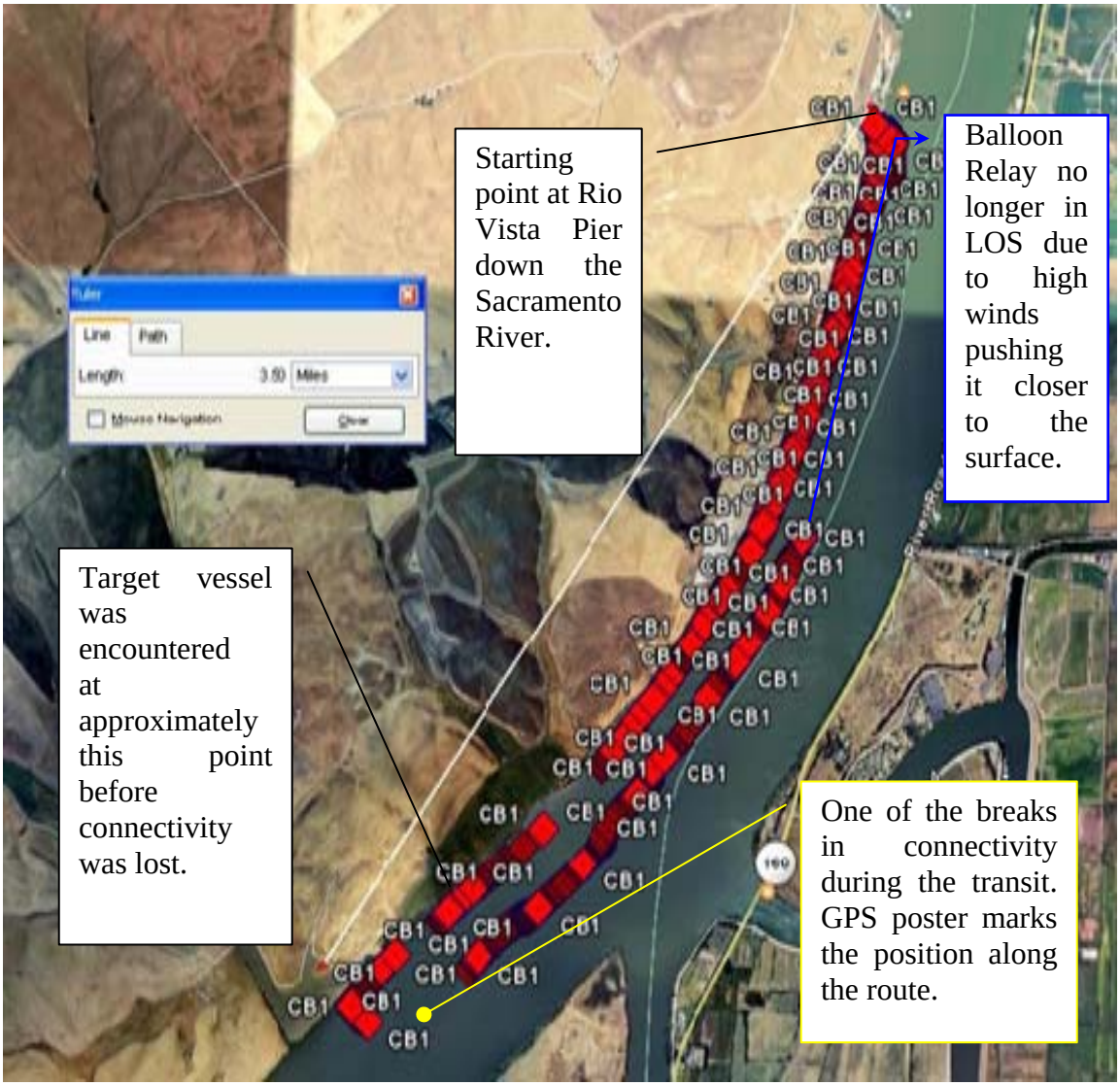

Figure 48. Google Earth View of Longest Distance Achieved in Riverine Area (After Bourakov, 2008)

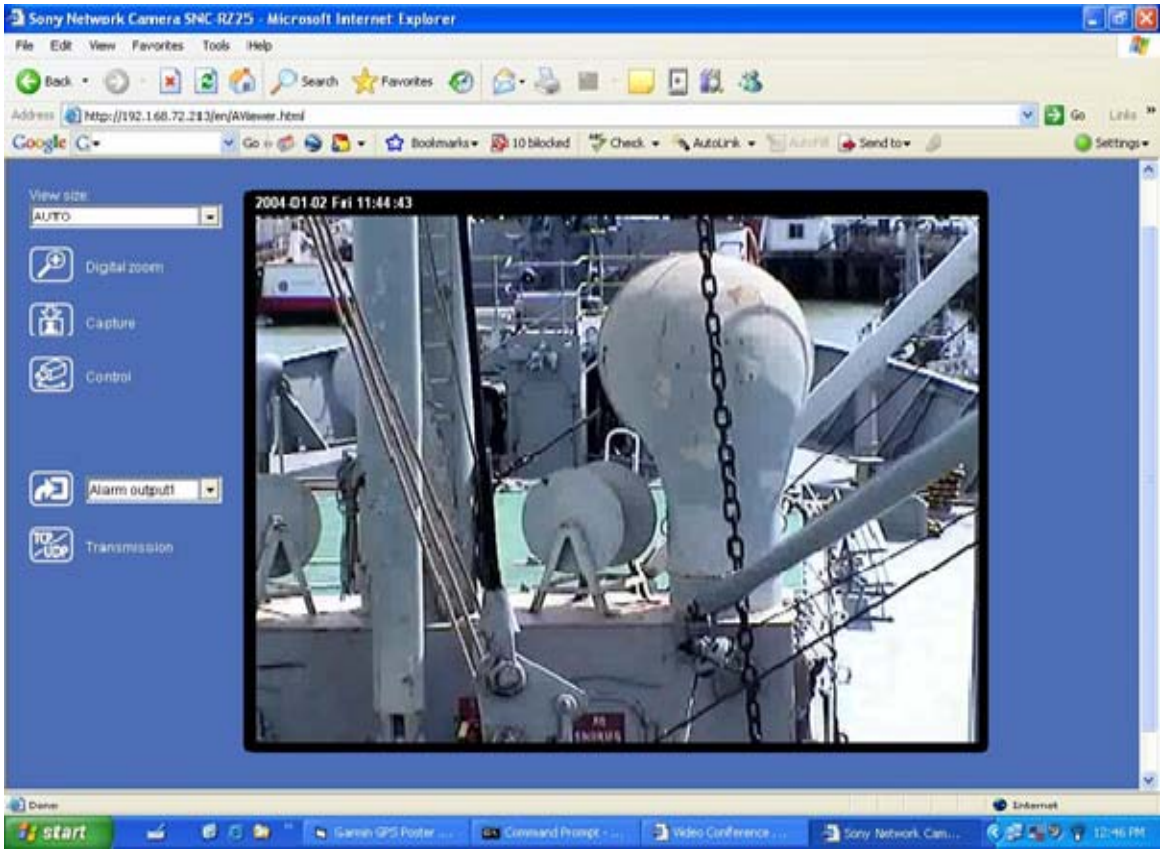

Figure 49. Snapshot from Riverine BP Laptop of Remote Target Vessel (From Bourakov, 2008)

Unfortunately, the biggest challenges were to keep the CB's laptop connected to the MIO network, by keeping the peripherals continuously connected and the Yagi antenna within LOS of the balloon relay. The other challenge was to conduct near real time sharing of the radiation files collected by LLNL personnel onboard the CB with the remote experts at LLNL for further analysis. However, due to the lack of a flash drive to download the files from the LLNL's laptop to the BP's laptop and lack of direct connectivity from the LLNL laptop on the CB to the 900 MHz link, the radiation data files could not be shared with remote experts until the CB returned to the pier. This in turn, kept the decision makers from being able to quickly act on the detection of radiation material onboard the TV. Furthermore, even if the flash drive was available, the high

winds were blowing the balloon relay further down to the surface, inhibiting a LOS path from the CB to the relay at the point of TV interdiction.

The only reliable form of real time communications left was the use of a cell phone. This method, however, was used only to update the TOC that the 900 MHz link was intermittent and that radiation files were captured to the LLNL laptop on board the CB. Since the LLNL laptop on the CB was only capable of storing and viewing data from the radiation sensor, there were no means available onboard to analyze the captured radiation data in order to take action, if necessary, or to inform LLNL or the TOC of what was suspected to be onboard the TV. In this respect, the data sharing tools failed to meet their full potential, due to a lack of communications link between the LLNL laptop and the remote experts at LLNL or the TOC.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

The results of the Vallejo Riverine Area MIO experiment were partially successful in that the 900 MHz link can still function in riverine areas as long as it is within LOS of the elevated relay as demonstrated by video capture of the S.F. bay TV. Additionally, at various times during the experiment, chat was available to the CB. Finally, the video streaming from the CB back to the video server at NPS and then back to the Riverine unit's laptop monitor also proved a successful network connection for the CB. Unfortunately, the USB connections for the GPS receiver and camera kept disconnecting when the Riverine unit hit choppy waters at a high speed. This problem can be resolved in the future by making the 900 MHz equipment into a self-contained unit.

Even though a test run of the setup was conducted at the ground station before the actual experiment began, and everything was checked to ensure that video and voice streaming were successful from the BO's laptop, there was no way to foresee the challenges posed once on the CB in riverine waters, especially the lack of a link of real time radiation data sharing between the LLNL laptop to LLNL. Also, the tethered balloon was getting blown down to a lower altitude due to high winds. This in turn cut our range down to approximately three and a half miles from the balloon relay. In less than windy conditions, it could have been possible to extend the range from the CB to the balloon relay. This strong winds and sea state are factors of operational conditions which cannot be ignored. Therefore, contingency plans to provide continuous connectivity to the network must include an alternate wireless path to the internet, like GSM.

The experiment turned out to prove that other collaborative tools are out there that can be used to augment Groove. Furthermore, the use of collaborative technology can prove to be very beneficial to military and civilian maritime interdiction forces. The tools were quite easy to set up and use. One of the problems was that the vast amounts of data were not properly labeled, used, or captured. The other problem observed was that too much information can pose a problem as much as no information when making a

decision. Furthermore, there is no need for everyone to see or have every bit of data available, as this only serves to congest their SA picture. Therefore, a better preparation of the information that needs to be received and analyzed needs to be a focus of the future efforts of data sharing during MIO experiments.

The reason this experiment was conducted the way it was is that the prior experiments had proven that it could be done again with the addition of more participating geographically distributed nodes. Furthermore, the new changes that were implemented were also tested either in the lab or at Camp Roberts prior to the MIO experiment. There are several factors which were not strongly considered prior to the experiment, which include which data was going to be seen by whom and how. However, this further shows how these collaborative tools can work in a Maritime environment even during rapid deployment. Therefore, the focus for the next MIO experiment is to have a more adaptive concept of operations to reflect the collaborative tools true potential to reinforce the features of each other and to enhance SA to expedite the decision-making process.

VI. FUTURE RECOMMENDATIONS

A. DATA SHARING

Data sharing between participating parties was also very hazy. The creation of a data manager position at each large participating node would help to clear up any further confusion prior, during, and after each experiment. This position could be developed in segments, in which there are two parts, one for the experiment and training and the other for real-world scenarios, which are implemented for single or multiple scenarios at a time.

For the Riverine portion of the MIO experiment, a lengthy pre-experiment discussion or brief among the members can be recommended. Of course, even though having an adaptive or flexible mindset is more realistic in most scenarios, it is necessary to be prepared for anything by having prior knowledge of what ship resources are available or not.

B. REDUNDANCY

For a redundant path, check GSM coverage along the river to provide multi-path option for data exchange. During the experiment, the BP was able to communicate with the TOC and remote TV via cellular phone because GSM coverage was good along the river. For future work, this could provide the alternate path when the 900 MHz link is not viable. This GSM option may not be available everywhere. Therefore, it is necessary to check if coverage is good, and only use it as a redundant path of data exchange. This implementation would require the use of a GPRS modem connected to the BP's laptop.

C. SEPARATION OF TASKS

A strong recommendation would be to separate NOC/TOC data management responsibilities by area of expertise. This would require a person handling nuclear radiation data to manage the distribution, invitations, storing, and displaying of that information to participants who need-to-know that information without cluttering their situational picture or congesting their data flow with superfluous data. A NOC commander or POC/OIC would be able to coordinate the various areas of responsibilities to ensure that data is always posted, retrieved, or gathered when needed without delaying the process by serving as the data manager. This idea would be very similar to a Navy ship's Combat Information Center layout, in which separate areas of warfare, i.e. air, surface, subsurface, strike, handle the management of their information and make it available upon request to the Tactical Action Officer, who is responsible for maintaining the operational situational awareness and acting upon it.

LIST OF REFERENCES

Adams, C., Meyer K., & Sundland J. (2008). Monitoring of the 802.16 OFDM Backbone for the CENETIX Network Including TNT and MIO Operations.

Bordetsky, A. & Friman, H. (2007). *Case-Studies of Decision Support Models for Collaboration in Tactical Mobile Environments.* 12th International Command and Control Research and Technology Symposium. Retrieved March 27, 2008, from http://www.dodccrp.org/events/12th_ICCRTS/CD/html/presentations/241.pdf.

Bourakov, E. (2008). MIO 08-2 Pictures downloaded to jump-drive.

Caldwell, S. L. (2006). *Maritime Security: Information-Sharing Efforts Are Improving*. (GAO-06-933T). United States Government Accountability Office. Retrieved April 5, 2008, from http://www.gao.gov/htext/d06933t.html.

CENETIX. (2006). After Action Report, TNT 06-3 MIO Experiment, (13-14 Jun 2006), from https://cenetix.nps.edu/ussocom/TNT_06-3/MIO%20AAR.doc.

CENETIX. (2007). After Action Report, TNT 07-2 MIO Experiment, (19-21 Mar, 2007), from https://cenetix.nps.edu/ussocom/TNT_07-2/MIO%2007-2.doc.

CENETIX. (2007). TNT 08-1 Quick Look Report. *Communications-on-the-move over SAOFDM*, from https://cenetix.nps.edu/ussocom/TNT_08-1/QLR%20SAOFDM%2008-1.doc.

CENETIX. (2007). After Action Report, TNT 07-1 MIO Experiment, (November 29-December 1, 2006), from https://cenetix.nps.edu/ussocom/TNT_07-1/MIO%20Final%20Report.doc.

CENETIX. (2007). After Action Report, TNT 07-3 MIO Experiment, (June 10-14, 2007), from https://cenetix.nps.edu/ussocom/TNT_07-3/MIO.doc.

CENETIX. (2007).After Action Report, TNT 07-4 MIO Experiment. Small Craft Interdiction and Collaboration on Radiation Awareness and Biometrics Identification, (September 10-13, 2007), from https://cenetix.nps.edu/ussocom/TNT_07-4/TNT_07-4_MIO.doc.

Collaborative Technologies, Maritime Interdiction Operation, Analysis of TNT 06-4. from https://cenetix.nps.edu/ussocom/TNT_06-4/IS4188%20-%20MIO%20Final%20Report.doc.

Defense Threat Reduction Agency. (2008). *About DTRA*. Retrieved April 9, 2008, from http://www.dtra.mil/about/mission/index.cfm.

Dougan, A. (2003). *Intermodal Cargo-Container Evaluation and Experimental Facility*.NNSA Office of Nonproliferation Research and Engineering (NA-22) Radiation Detection Technologies Program R&D Portfolio, Retrieved April 8, 2008, from http://rdc.llnl.gov/rdp/intermodal.html.

Farrell, M. M. (2006). *Expansion of the Center For Network Innovation And Experimentation (CENETIX) Network To A Worldwide Presence.* Master's Thesis, Naval Postgraduate School, Monterey, California.

Gayman, R. (2004). *Coast Guard Takes on Drug Smugglers in the Eastern Pacific*. Retrieved April 6, 2008, from http://www.uscgsanfrancisco.com/go/doc/823/65657/.

Harahan, J. P. & Bennett, R. J. (2002). *Creating The Defense Threat Reduction Agency (DTRA History Series)*. Virginia: U.S. Department of Defense.

Harbaugh, E. E. (2004).*The Proliferation Security Initiative: Counterproliferation at the Crossroads*. Strategic Insights, III, Retrieved April 6, 2008, from http://www.ccc.nps.navy.mil/si/2004/jul/harbaughJul04.asp.

Keel, P. et al. (2004). *EWALL electronic Card Wall Introduction*. Retrieved April 8, 2008, from http://ewall.mit.edu/introduction/.

Klopson, J. E. & Burdian, S. V. (2005). *Collaborative Applications Used In A Wireless Environment At Sea For Use In Coast Guard Law Enforcement And Homeland Security Missions*. Master's Thesis ,Naval Postgraduate School, Monterey, California.

Lawrence Livermore National Laboratory. (2007). *Science and Technology Benefitting the State of California*. Retrieved April 8, 2008, from https://publicaffairs.llnl.gov/news/fact_sheets/science_highlights.pdf.

Marvin, C. (2005). *802.16 OFDM Rapidly Deployed Network For Near-Real-Time Collaboration Of Expert Services In Maritime Security Operations*. Master's Thesis, Naval Postgraduate School, Monterey, California.

McKenna, H. (2001). *Collaborative Planning Solutions: Using USMC Standard Collaboration Tools to Assist with Mission Planning and Execution.* Master's Thesis, Naval Postgraduate School, Monterey, California.

Netzer, D. (2008). *Email: Subject: Pictures of MIO 08-2.*, from: dnetzer@nps.edu.

Office of the Inspector General. (2006). *The Federal Bureau of Investigation's Efforts to Protect the Nation's Seaports.* Retrieved April 5, 2008, from http://www.usdoj.gov/oig/reports/FBI/a0626/exec.htm.

Report on Stiletto Integration and in TNT 06-4 MIO Experiment and Networking Node Development. (August 30-September 1, 2006), from https://cenetix.nps.edu/ussocom/TNT_06-4/Stiletto%20Integration.doc.

Schwoegler D. (2006). *Marine Experiment Tests Detection Capability*. Newsline, 31, 4.

Stavroulakis, G. (2006). *Rapidly Deployable, Self Forming, Wireless Networks For Maritime Interdiction Operation.* Master's Thesis, Naval Postgraduate School, Monterey, California.

U.S. Department of Energy. (2005) *Radiological Assistance Program (RAP).* U.S. Department of Energy, National Nuclear Security Administration, Retrieved April 15, 2008, from http://www.nv.doe.gov/library/FactSheets/RAP.pdf.

U.S. Environmental Protection Agency. (2007) National Response Center. Retrieved April 8,2008, from http://www.epa.gov/superfund/programs/er/nrs/nrsnrc.htm.

USSOCOM/NPS Field Experimentation Program, Tactical Network Topologies 06-01. 14-18, 20-22 November 2005. After Action Report 10 January 2006. from https://cenetix.nps.edu/ussocom/TNT_06-1_AAR.doc.

USSOCOM/NPS Field Experimentation Program, Tactical Network Topologies 06-02 After Action Report. Alameda, CA from 5-7 March 2006. from https://cenetix.nps.edu/ussocom/TNT_06-2_AAR.doc.

USSOCOM/NPS Field Experimentation Program, Tactical Network Topologies 06-03, After Action Report. 2006. from https://cenetix.nps.edu/ussocom/TNT_06-3_AAR.pdf.

USSOCOM/NPS Field Experimentation Program, Tactical Network Topologies 06-4 After Action Report. 2006. from https://cenetix.nps.edu/ussocom/TNT_06-4_AAR.doc.

USSOCOM-NPS Field Experimentation Cooperative Program, Tactical Network Topologies 07-01. After Action Report 2007. from https://cenetix.nps.edu/ussocom/TNT_07-1_AAR.doc.

USSOCOM-NPS Field Experimentation Cooperative Program, Tactical Network Topologies 07-02. After Action Report 2007. from https://cenetix.nps.edu/ussocom/TNT_07-2_AAR.doc.

USSOCOM-NPS Field Experimentation Cooperative Program, Tactical Network Topologies 07-3. After Action Report 2007. from https://cenetix.nps.edu/ussocom/TNT_07-3_AAR.doc.

USSOCOM-NPS Field Experimentation Cooperative Program, Tactical Network Topologies 07-04. After Action Report 2007. from https://cenetix.nps.edu/ussocom/TNT_07-4_AAR.doc.

West Virginia Biometrics Initiative. (2008). *Department of Defense Biometrics Fusion Center*. Retrieved March 28, 2008. from http://www.wvbiometrics.org/department-of-defense-biometrics-fusion-center.html/.

Wikipedia The Free Encyclopedia. (2008). United States Coast Guard. Retrieved April 8, 2008, from http://en.wikipedia.org/wiki/USCG.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alexander Bordetsky
   Naval Postgraduate School
   Monterey, California

4. Eugene Bourakov
   Naval Postgraduate School
   Monterey, California

5. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Albert Mercado
   Naval Postgraduate School
   Monterey, California